Centre Microsoft de gestion de la confidentialité

Réponses sur l'évaluation du GDPR

Août 2017

Dédit de responsabilité

Ce livre blanc commente le Règlement général sur la protection des données (GDPR) selon son interprétation faite par Microsoft, à la date de cette publication. Nous avons passé beaucoup de temps sur ce règlement et nous avons étudié très sérieusement ses intentions et sa signification. Mais l'application du GDPR dépend largement de faits spécifiques et toutes les interprétations et tous les aspects du GDPR ne sont pas tous bien établis.

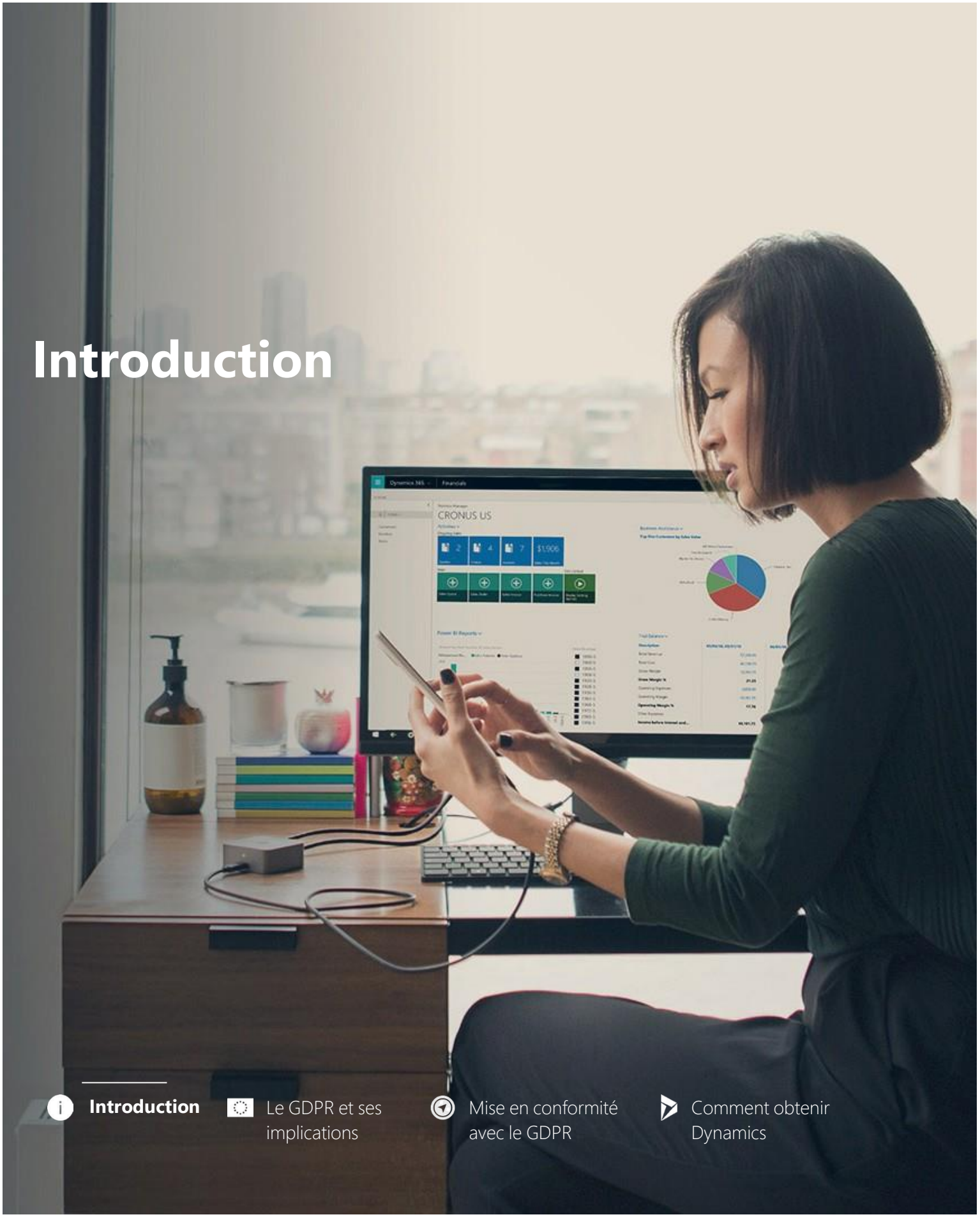
Par conséquent, ce livre blanc n'est fourni qu'à titre d'information et ne doit pas être considéré comme un conseil juridique ; il ne permet pas de déterminer comment le GDPR doit s'appliquer dans votre cas, dans votre organisation. Nous vous conseillons de travailler avec un conseil juridique spécialisé dans ce domaine afin d'étudier avec lui le GDPR, son application spécifique dans le cadre de votre organisation et les mesures à prendre pour être en conformité.

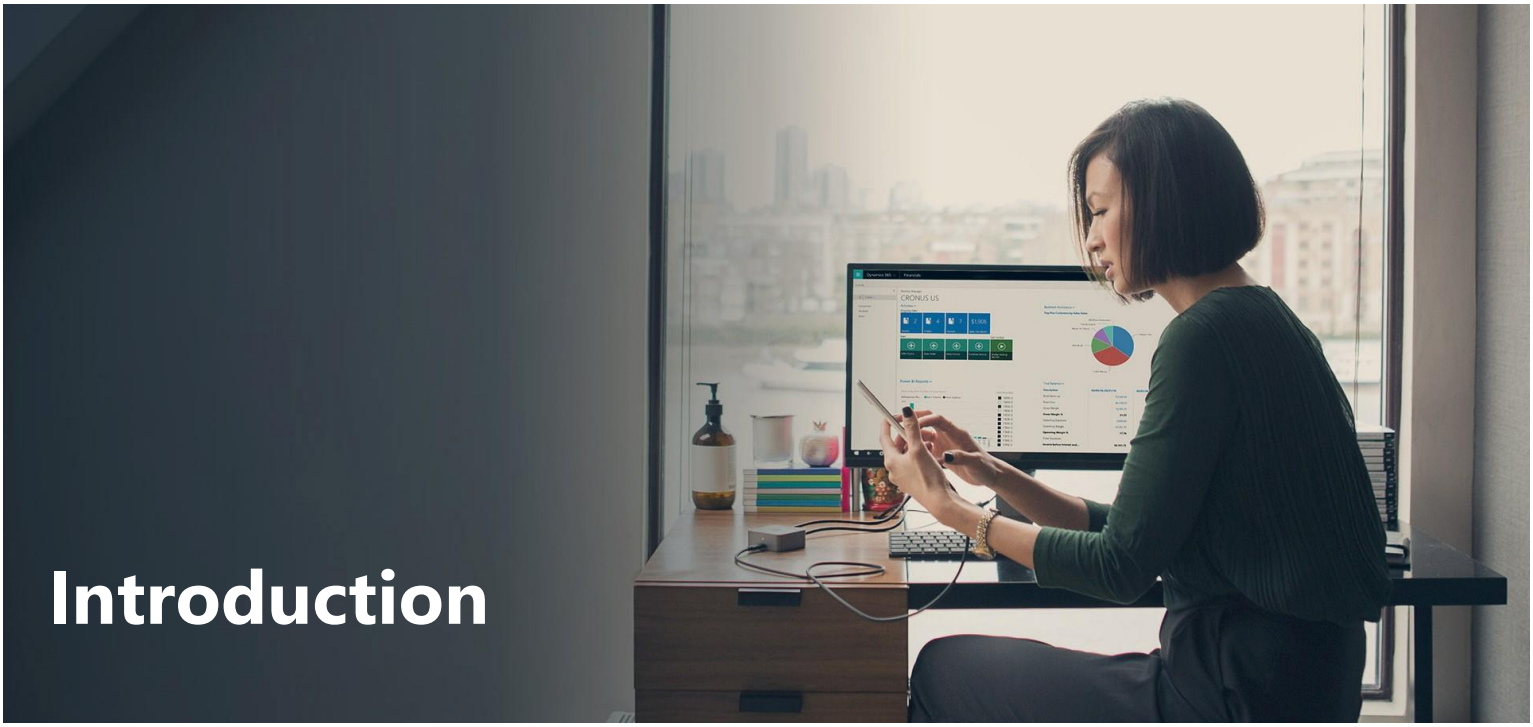
MICROSOFT EXCLUT TOUTE GARANTIE, EXPRESSE, IMPLICITE OU STATUTAIRE, EN CE QUI CONCERNE CE DOCUMENT. Ce document est fourni en l'état. Les informations et opinions fournies ici, y compris les URL et les références aux sites Internet, peuvent être modifiées à tout moment sans avis préalable.

Ce document n'a pas pour effet de vous concéder une quelconque licence sur la propriété intellectuelle des produits Microsoft. Vous pouvez copier et utiliser ce document uniquement dans le cadre d'une utilisation interne à votre entreprise.

Sommaire

Introduction





Introduction

Introduction

Le 25 mai 2018, un nouveau règlement européen sur la protection des données s'appliquera et définira une nouvelle référence globale pour les droits au respect de la vie privée, la sécurité des données et la conformité.

Le Règlement Général sur la Protection des Données (RGPD ou GDPR en anglais) vise à protéger et à renforcer les droits de la vie privée des personnes. Le GDPR définit des conditions strictes sur la façon de gérer et de protéger des données personnelles tout en respectant les choix de chacun, indépendamment du lieu où les données sont transmises, traitées ou stockées.

Microsoft et ses clients doivent désormais atteindre les objectifs du GDPR concernant le respect de la vie privée. Chez Microsoft, nous pensons que la vie privée est un droit fondamental ; le GDPR constitue une étape importante pour avancer dans la clarification et la mise en place des droits relatifs à la vie privée. Mais nous pensons aussi que le GDPR imposera des modifications importantes pour beaucoup d'entreprises dans le monde.

Nous avons montré notre engagement à soutenir le GDPR et nous voulons apporter à nos clients de l'aide. Pour cela, notre Responsable de la vie privée, Brendon Lynch, tient un blog « Get GDPR compliant with the Microsoft Cloud » (Conformité du Microsoft Cloud avec le GDPR) et Rich Sauer, Vice-Président de Microsoft et Avocat conseil, gère un blog « Earning your trust with contractual commitments to the General Data Protection Regulation » (Gagner votre confiance avec des engagements contractuels envers le GDPR).

Bien que la mise en œuvre du GDPR dans votre organisation puisse être délicate, nous sommes là pour vous aider. Pour obtenir des informations spécifiques sur le GDPR, nos engagements et la marche à suivre, veuillez visiter la section GDPR du Centre Microsoft de gestion de la confidentialité.

Liens

Blog « Get GDPR compliant with the Microsoft Cloud »

BLOG

Lire les autres billets de Brendon Lynch

BRENDON LYNCH

Blog « Earning your trust with contractual commitments to the General Data Protection Regulation »

BLOG

Lire les autres billets de Rich Sauer

RICH SAUER

Visiter la section GDPR du Centre Microsoft de gestion de la confidentialité

CENTRE DE GESTION DE LA CONFIDENTIALITÉ

Le GDPR et ses implications

Données personnelles et sensibles

- Définitions des données
- Pseudonymisation des données
- Données Dynamics 365

Le GDPR et ses implications

Le GDPR est un document juridique qui décrit la mise en œuvre de la Stratégie numérique pour un marché unique. C'est un règlement complexe qui peut entraîner des changements importants dans la façon selon laquelle vous collectez, utilisez et gérez des données. Depuis longtemps, Microsoft aide ses clients à se conformer à des législations complexes et nous serons votre partenaire dans votre préparation à intégrer le GDPR dans votre organisation.

Le GDPR impose de nouvelles règles aux entreprises qui offrent des biens et des services aux personnes résidant dans l'Union Européenne (UE), ou qui collectent et analysent des données liées à des résidents de l'UE, quel que soit le lieu où ces entreprises sont installées. Parmi tous les points décrits par le GDPR, voici les principaux :

- **Amélioration du respect des droits de la vie privée :** renforcement de la protection des données pour les personnes au sein de l'Union Européenne (UE) en leur donnant les droits d'accéder à leurs données, de corriger des inexactitudes, d'effacer des données, de déplacer leurs données et de s'opposer au traitement de leurs informations.
- **Renforcement de la protection des données :** renforcement de la responsabilité des entreprises et des établissements du secteur public qui traitent des données personnelles, renforcement de leur responsabilité afin de conformer à ce règlement.
- **Signalement obligatoire des violations de données :** les entreprises doivent signaler toutes violations de données auprès de leurs autorités de tutelle sans délai, et si possible en moins de 72 heures.
- **Pénalités importantes en cas de non-respect de ce règlement :** des sanctions élevées, incluant des amendes substantielles, seront appliquées si une entreprise a, de façon intentionnelle ou par inadvertance, manqué à ses obligations.

Par conséquent, le GDPR peut avoir un impact significatif sur votre entreprise. Il peut vous obliger à revoir vos politiques en matière de vie privée, à implanter ou à renforcer vos contrôles sur la protection des données et sur les procédures de notifications en cas de violations de données, à déployer des politiques transparentes et à investir dans votre service informatique et la formation.

Liens

Pour en savoir plus sur la Stratégie numérique du marché unique

SITE WEB >

Le GDPR et ses implications

Le GDPR couvre toutes les opérations des responsables de traitements et des sous-traitants dans l'UE, et de ceux, à l'extérieur de l'UE, qui offrent des biens et des services, ou qui collectent des données personnelles, des résidents de l'UE. Le GDPR clarifie aussi certains éléments en relation avec les types de données à protéger. Enfin, il met en place un mécanisme additionnel pour poursuivre en justice toutes les entreprises en infraction.

Données personnelles et sensibles

Définitions des données

Afin de vous placer en conformité avec le GDPR, vous devez comprendre à la fois les définitions des données personnelles et des données sensibles, et leur relation avec les types de données gérées par votre organisation avec Dynamics 365. Après cela, vous serez à même de comprendre comment les données sont créées, traitées, gérées et stockées.

Le GDPR considère comme donnée personnelle, toute information relative à une personne naturelle identifiée ou identifiable. Cela peut inclure à la fois des informations directes (par exemple, votre nom légal) et des informations indirectes (des informations qui permettent votre identification sans qu'elles ne soient associées directement à votre nom).

Le GDPR indique sans équivoque que le concept de données personnelle inclut des identificateurs en ligne (par exemple, adresse IP, identifiant d'appareil mobile) et des données de géolocalisation, alors que la précédente Directive de protection des données de l'UE était moins explicite.

Les données personnelles sensibles bénéficient de protections renforcées et généralement, nécessitent le consentement explicite de la personne sur le lieu de traitement de ces données.

Pseudonymisation des données

Le GDPR décrit aussi le concept de données pseudonymes qui permettent l'identification d'une personne par le recours à des informations supplémentaires. Ce concept est différent de celui de données anonymes, pour lesquelles le lien direct avec la personne concernée est détruit. Avec des données anonymes, il n'est pas possible de retrouver le titulaire de la donnée ; le GDPR ne s'applique pas à ces données. Toutefois, les données de ce type sont rarement utiles dans vos applications.

Comme indiqué dans le GDPR (préambule §28) : « La pseudonymisation des données à caractère personnel peut réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à remplir leurs obligations en matière de protection des données. L'introduction explicite de la pseudonymisation dans le présent règlement ne vise pas à exclure toute autre mesure de protection des données. »

Exemples d'informations relatives à une personne naturelle identifiée ou identifiable

- Nom
- Identification (par ex., n° de sécurité sociale)
- Données de localisation géographique (par ex., adresse du domicile)
- Identificateur en ligne (par ex., adresse email, adresse IP, nom à l'écran, identifiants d'appareils).

Pour utiliser la pseudonymisation, vous pouvez par exemple utiliser un jeton obtenu dans une table séparée qui fait la liaison entre la personne et un numéro d'identification généré de façon aléatoire. (Par ex., « 12345 » est l'identificateur de « Jean Dupont ».) Vous pouvez aussi utiliser le chiffrement des données : un algorithme mathématique sert à protéger les données de la personne. Si vous perdez le jeton ou la clé de chiffrement, il vous reste essentiellement des données anonymes.

Le GDPR encourage la pseudonymisation afin de renforcer la sécurité ; c'est une mesure qui renforce la protection de la vie privée.

Vous serez fortement incité à utiliser des mesures de protection techniques et organisationnelles des données dans le cadre du GDPR, afin d'atténuer vos obligations en matière de conformité et de gestion des risques. Gardez à l'esprit que le GDPR considère le chiffrement et la pseudonymisation comme des mesures de protection garantissant le maintien d'un niveau de sécurité adapté au risque ; d'ailleurs, l'article 34 précise que la notification à la personne concernée par une faille dans la protection de données protégées peut être évitée si « le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées (...) telles que le chiffrement ».

Données Dynamics 365

En tenant compte de la définition des données telle qu'elle est faite dans le GDPR, passons en revue les données gérées dans Dynamics 365. Microsoft définit des types de données spécifiques à ses services en ligne, tels que Dynamics 365, dans sa Charte de confidentialité en ligne. Comme indiqué ci-dessous, certaines de ces données seront sous votre responsabilité car vous devez gérer vos données d'une façon conforme à ce que décrit le GDPR. Cette liste vous permet d'effectuer un premier passage en revue de vos données :

- **Les données des clients** sont toutes les données, y compris les textes, les enregistrements audio et vidéo, les images et les logiciels que vous fournissez à Microsoft ou qui sont fournis en votre nom pour être utilisés dans des services en ligne professionnels de Microsoft. Par exemple, il s'agit des données que vous téléversez sur les systèmes de Microsoft à des fins de stockage ou de traitement, ainsi que les applications que vous téléversez à des fins de distribution via un service professionnel du Cloud Microsoft. Ces données peuvent potentiellement contenir des données personnelles régies par le GDPR.
- **Le contenu client** est un sous-ensemble des données des clients. Il s'agit généralement de données confidentielles qui, dans le cadre du fonctionnement normal du service, ne sont pas transmises sur Internet sans être chiffrées. Par exemple, il peut s'agir d'emails avec des pièces jointes, du contenu de sites SharePoint en ligne (pas d'URL), du contenu de fichiers, de messages instantanés, de communications vocales et de fichiers CRM contenant des données sur les interactions avec vos clients. Ces données peuvent potentiellement contenir des données personnelles régies par le GDPR.

Lien

Lire la Charte de confidentialité en ligne de Microsoft

CHARTE DE CONFIDENTIALITÉ

- **Les données d'administrateur** sont les données sur les administrateurs, fournies lors de la signature du contrat, de l'achat ou de l'administration des services Microsoft, comme des noms, des numéros de téléphone et des adresses email. Cela inclut aussi des données et des informations liées à votre compte, comme les contrôles que vous sélectionnez. Nous utilisons les données d'administrateur pour fournir des services, terminer des transactions, servir le compte et détecter des fraudes éventuelles. Ces données pouvant contenir des données personnelles d'une personne, elles peuvent rentrer dans le cadre d'application du GDPR.
- **Les données de paiement** sont les informations que vous fournissez lorsque vous effectuez des achats en ligne chez Microsoft. Il peut s'agir d'un numéro de carte de crédit et d'un code de sécurité, d'un nom et d'une adresse de facturation, et d'autres données financières. Nous utilisons les données de paiement pour terminer des transactions et détecter des fraudes éventuelles. Certaines de ces données pouvant être associées à une personne plutôt qu'à une entreprise (par exemple, paiement avec une carte bancaire personnelle au lieu d'utiliser une carte bancaire de l'entreprise), elles entrent dans le cadre d'application du GDPR.
- **Les données de support** sont les informations que nous collectons lorsque vous contactez Microsoft pour demander de l'aide, comme les informations que vous fournissez dans une demande de support, les rapports d'un outil de dépannage automatique ou les fichiers que vous nous transmettez. Les données de support n'incluent pas de données financières mais elles peuvent contenir des informations d'administration pour suivre un ticket enregistré dans nos systèmes.

En plus des types de données que nous venons de citer et des données personnelles décrites dans la section précédente, il existe des conditions spécifiques relatives aux enfants. Comme l'indique le GDPR, les enfants (définis comme personnes naturelles de moins de 16 ans ou d'un autre âge selon les lois de chaque État membre), doivent bénéficier d'une protection spécifique sur leurs données personnelles. Comme ces données peuvent être en relation avec des données client et/ou des données de contenu dans Dynamics 365 selon les définitions ci-dessus, vous devrez, en tant que responsable, obtenir le consentement du représentant légal de chaque enfant pour l'utilisation de données personnelles.

Mise en conformité avec le GDPR

Les 4 étapes à suivre

- Découvrir
- Administrer
- Protéger
- Signaler

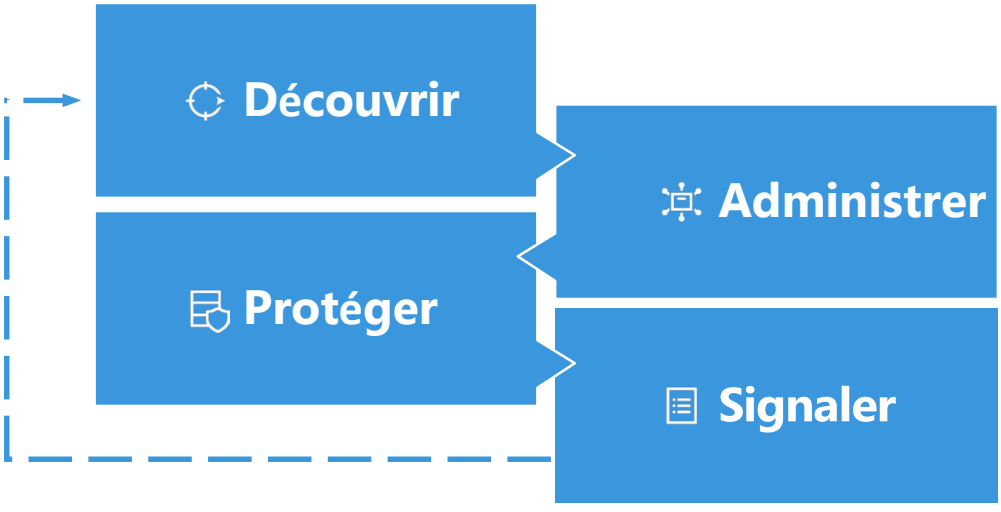
Mise en conformité avec le GDPR

Les 4 étapes à suivre

Par où devez-vous commencer ? Comment vous y prendre pour être en conformité avec le GDPR dans les applications Dynamics 365 que vous utilisez ?

Dans le livre blanc « Beginning your General Data Protection Regulation (GDPR) Journey », nous abordons des thèmes comme une présentation de GDPR, l'impact de cette règlementation sur votre entreprise et comment vous devez aborder votre transformation dès aujourd'hui. Nous vous recommandons de commencer votre mise en conformité avec le GDPR en vous concentrant sur quatre étapes principales :

- **Découvrir :** identifiez les données personnelles que vous gérez et leur lieu de stockage.
- **Administrer :** déterminez comment les données personnelles sont utilisées et par qui.
- **Protéger :** mettez en place des contrôles de sécurité pour empêcher et détecter des vulnérabilités et des violations de données, et pour y répondre.
- **Signaler :** produisez des rapports en cas de violations de données et conservez toutes les informations requises.



Lien

Lire le livre blanc « Beginning your General Data Protection Regulation (GDPR) Journey » (en anglais)

LIVRE BLANC

Principales étapes GDPR

Découvrir : identifiez les données personnelles que vous gérez et leur lieu de stockage.

Administrer : déterminez comment les données personnelles sont utilisées et par qui.

Protéger : mettez en place des contrôles de sécurité pour empêcher et détecter des vulnérabilités et des violations de données, et pour y répondre.

Signaler : produisez des rapports en cas de violations de données et conservez toutes les informations requises.

Découvrir

Identifiez les données personnelles que vous gérez et le lieu où elles sont stockées.

Le GDPR impose de nombreuses conditions sur la collecte, le stockage et l'utilisation de données personnelles. Il est donc essentiel de commencer par identifier les données personnelles que vous possédez sur les personnes concernées. Après avoir identifié les données que vous stockez et que vous utilisez, vous devez classez toutes les données personnelles que vos utilisateurs ont le droit de consulter, à condition qu'ils aient les autorisations nécessaires selon le GDPR.

Rechercher et identifier des données personnelles

Le GDPR impose de nombreuses conditions sur la collecte, le stockage et l'utilisation de données personnelles. Il est donc essentiel de commencer par identifier les données personnelles que vous possédez sur les personnes concernées.

Approche Dynamics 365 : Microsoft Dynamics 365 fournit plusieurs méthodes pour vous permettre de rechercher des données personnelles dans vos enregistrements, comme la Recherche avancée, la Recherche immédiate et la Recherche par pertinence. Ces fonctions vous permettent d'identifier très rapidement et avec précision des données personnelles.

Faciliter la classification des données

Le GDPR impose de nouvelles conditions qui renforcent les droits des personnes concernées. Par conséquent, il est nécessaire de classer les données personnelles.

Approche Dynamics 365 : La plateforme Dynamics 365 offre la flexibilité de construire une extension d'application pour la classification des données, par exemple au niveau d'un champ ou d'une entité. À ces niveaux, les clients peuvent configurer des formulaires et des vues pour chercher des informations personnelles selon les critères du GDPR. Au niveau des lignes, la classification des données est obtenue via une personnalisation de la solution.

Questions à étudier

Combien de données personnelles sur les personnes concernées avez-vous identifiées dans votre organisation ?

Quelle confiance accordez-vous aux outils que votre organisation emploie actuellement pour classer les données personnelles ?

Mise en conformité avec le GDPR

Administrer

Administrer

Déterminez comment les données personnelles sont utilisées et par qui.

La meilleure pratique de gestion des données dans le cadre du GDPR consiste à implanter un programme de gouvernance organisationnelle qui permet de notifier aux personnes concernées le traitement prévu de leurs données personnelles, d'obtenir leur consentement sur ce traitement, de fournir un mécanisme à ces personnes pour qu'elles puissent demander l'arrêt de ce traitement, la correction de données inexactes, l'ajout de données personnelles, le transfert ou l'effacement de ces données. Votre programme de gestion des données doit aussi indiquer comment ces demandes seront traitées, suivies et fermées.

Selon le GDPR, les personnes concernées ont droit à la portabilité des données : elles peuvent demander et recevoir leurs données personnelles dans un format structuré, standard, lisible par une machine. Enfin, votre organisation doit être capable de restreindre le traitement des données suite à une demande de restriction temporaire sur certains traitements de la part des personnes concernées.

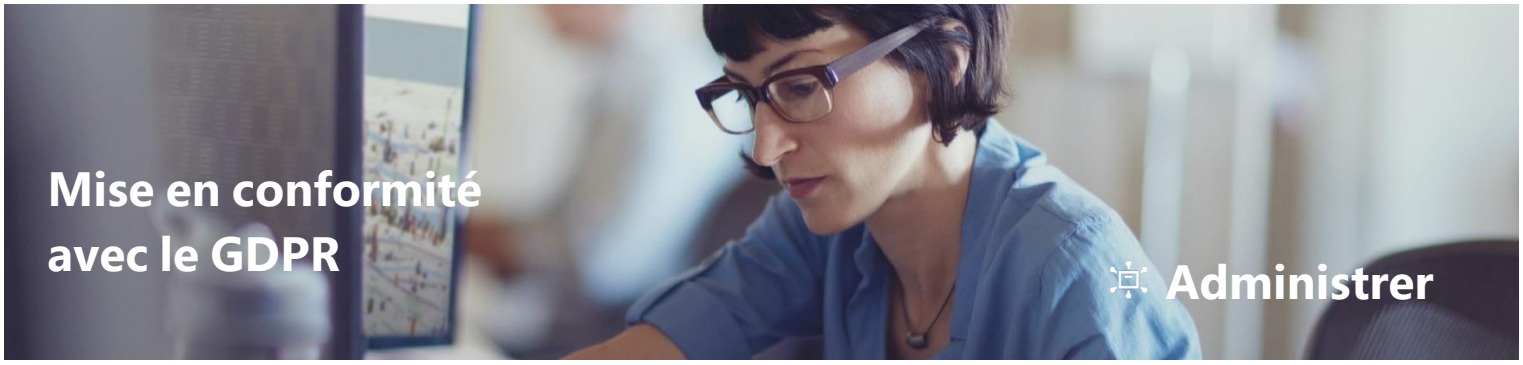
Activer des procédures et des pratiques de gouvernance des données

Pour gérer les données et prendre en compte les droits des personnes concernées selon les définitions du GDPR, les organisations doivent mettre en place un programme de gouvernance des données.

Approche Dynamics 365 : Dynamics 365 fournit de nombreuses fonctionnalités pour gérer l'accès aux données personnelles. Dynamics 365 utilise Azure Active Directory pour protéger vos données d'un accès non autorisé, en simplifiant la gestion des utilisateurs et des groupes et en facilitant la tâche des administrateurs pour assigner ou révoquer des droits. La sécurité basée sur des rôles vous permet de grouper des droits afin de limiter les tâches qu'un utilisateur peut réaliser. La sécurité basée sur les enregistrements vous permet de restreindre l'accès de certains enregistrements. La sécurité au niveau des champs vous permet de restreindre l'accès de certains champs tels que ceux contenant des informations liées à des personnes identifiables.

Questions à étudier

Votre organisation a-t-elle mis en place un programme de gouvernance des données qui répond aux demandes du GDPR ?



Fournir une information détaillée sur les activités de traitement aux personnes concernées

Vos notifications actuelles relatives à la vie privée répondent-elles aux exigences du GDPR ?

Le GDPR demande que les responsables des traitements soient transparents envers les personnes concernées en ce qui concerne le traitement prévu de leurs données personnelles.

Approche Dynamics 365 : Dynamics 365 permet d'afficher des notifications personnalisées relatives à la vie privée, contenant des informations détaillées. Ces informations peuvent être affichées dans un formulaire ou sur l'écran d'ouverture de session des portails interne et externe. Dynamics 365 peut ainsi afficher des notifications sur des sites ouverts au public mais c'est de votre responsabilité de vérifier que la langue utilisée dans la notification répond aux obligations définies dans le GDPR.

Arrêter un traitement sur demande

Votre organisation est-elle vraiment capable d'arrêter un traitement sur demande ?

Le GDPR impose que les organisations donnent aux personnes concernées le droit de s'opposer au traitement de leurs données et de demander l'arrêt du traitement de leurs données.

Approche Dynamics 365 : Dynamics 365 propose plusieurs outils pour vous permettre d'arrêter un traitement sur demande. Des outils comme la Recherche avancée, la Recherche rapide et la Recherche par pertinence vous permettent de bloquer manuellement un traitement dans Dynamics 365, y compris des analyses de texte et marketing.

Collecter un consentement sans ambigüité auprès des personnes concernées

Dans combien de cas votre organisation est-elle vraiment capable d'obtenir un consentement nécessaire ?

Avant tout traitement de données, le GDPR demande aux responsables du traitement d'avoir le droit d'effectuer un tel traitement, c'est-à-dire de collecter le consentement explicite des personnes concernées.

Approche Dynamics 365 : Dynamics 365 propose des portails qui permettent de demander et d'obtenir le consentement des personnes avant de traiter leurs données. Lors de la collecte de données personnelles, Dynamics 365 vous permet de créer des cases à cocher et d'autres éléments qui permettent aux personnes concernées d'indiquer de façon affirmative et explicite qu'elles acceptent le traitement de leurs données personnelles. Dynamics 365 peut ainsi afficher des notifications sur des sites ouverts au public mais c'est de votre responsabilité de vérifier que la langue utilisée dans la notification répond aux obligations définies dans le GDPR.

Faciliter les demandes de rectification, d'effacement ou de transfert de données personnelles

Votre organisation est-elle vraiment capable de proposer un moyen pour que les personnes concernées puissent exprimer ces demandes et que ces demandes soient prises en compte ?

Le GDPR impose que le responsable du traitement de données personnelles fournisse aux personnes concernées un moyen pour demander de rectifier, d'effacer ou de transférer leurs données personnelles.

Approche Dynamics 365 : Dynamics 365 propose aux utilisateurs plusieurs outils pour effacer et modifier des données personnelles associées aux personnes concernées ainsi qu'aux comptes des employés. Les utilisateurs peuvent manuellement suivre les demandes de modification, d'effacement ou de transfert de données personnelles ; ils peuvent créer des rapports pour suivre et administrer les demandes des personnes concernées. De plus, les actions prises pendant la durée de la demande peuvent être suivies, et la demande peut être marquée comme état résolue lorsqu'elle est terminée. Via les portails, les administrateurs des contrats clients Dynamics 365 peuvent recevoir des demandes concernant les données personnelles.

Rectifier sur demande des données personnelles inexactes ou incomplètes

Votre organisation peut-elle vraiment rectifier des données personnelles inexactes ou incomplètes si une personne concernée vous le demande ?

Le GDPR impose au responsable du traitement que les personnes concernées puissent demander la rectification de données personnelles inexactes ou incomplètes.

Approche Dynamics 365 : Dynamics 365 propose plusieurs méthodes pour rectifier des données personnelles inexactes ou incomplètes. Avec Excel Online, vous pouvez exporter, modifier en masse puis réimporter des lots d'enregistrements dans Dynamics 365. Vous pouvez modifier des données personnelles enregistrées dans Contacts en modifiant manuellement les données concernées. Vous pouvez aussi modifier une ligne seule ou modifier plusieurs lignes directement en utilisant des formulaires Dynamics 365.

Effacer des données personnelles sur demande

Votre organisation peut-elle vraiment gérer une demande d'effacement des données personnelles ?

Selon le GDPR, toutes les personnes concernées ont le droit de demander l'effacement de leurs données personnelles auprès du responsable du traitement.

Approche Dynamics 365 : Dynamics 365 propose plusieurs méthodes pour effacer des données personnelles. Avec des outils comme la Recherche avancée, vous pouvez identifier facilement des données personnelles et les effacer directement.

Fournir à la personne concernée ses données personnelles sous une forme structurée et standard

Si une personne concernée demande à recevoir ses données personnelles, votre organisation est-elle capable de répondre à cette demande ?

Selon le GDPR, toutes les personnes concernées ont le droit à la portabilité des données. Cela signifie qu'elles peuvent demander leurs données personnelles auprès du responsable du traitement, et les recevoir dans un format courant, structuré, lisible par un ordinateur.

Approche Dynamics 365 : Les données Dynamics 365 peuvent être exportées vers un fichier Excel statique afin de faciliter le portage des données. Avec Excel, vous pouvez ensuite modifier les données personnelles qui seront incluses dans la réponse, puis enregistrer les données sous un format courant, lisible par un ordinateur, tel que .CSV ou .xml.

Restreindre le traitement des données personnelles

Selon le GDPR, les personnes concernées peuvent demander, dans certaines circonstances, une limitation de traitement de leurs données. Cela peut aussi être le cas si la personne concernée s'oppose au traitement de ses données, mais le responsable du traitement a des obligations légales de conservation des données pendant un certain temps. Par conséquent, le responsable du traitement peut avoir besoin de moyens techniques pour empêcher les données personnelles spécifiques d'une personne concernée d'être prises en compte dans certains traitements.

Approche Dynamics 365 : Pour protéger les informations sensibles et permettre la suspension d'un traitement comme le demande le GDPR, Dynamics 365 intègre des mesures de sécurité aux niveaux de la plateforme et du service. Dynamics 365 propose plusieurs outils pour aider à limiter le traitement de données personnelles, comme la Recherche avancée, la Recherche rapide ou la Recherche par pertinence, pour trouver manuellement les données concernées et limiter leur traitement.

Votre organisation est-elle capable vraiment de répondre à une demande d'une personne concernée pour limiter le traitement de ses données personnelles ?

Protéger

Mettez en place des contrôles de sécurité pour empêcher et détecter des vulnérabilités et des violations de données, et pour y répondre.

Vos activités de traitement et la technologie sous-jacente doivent intégrer des contrôles de sécurité et de respect de la vie privée qui assurent la disponibilité, l'intégrité et la confidentialité des données personnelles. Le chiffrement est une solution potentielle qui peut répondre aux exigences du GDPR en ce qui concerne un haut niveau de sécurité. Si une violation de données se produit, dès lors que vous en avez connaissance, vous devez avertir rapidement les régulateurs et il est possible que vous deviez aussi avertir les personnes concernées. Des tests et une évaluation de l'efficacité de vos mesures de sécurité organisationnelles et techniques doivent être régulièrement effectués pour vous assurer que vous protégez correctement les données personnelles.

Protection des données et respect de la vie privée par conception et par défaut

Le GDPR demande aux responsables des traitements ou à leurs sous-traitants qui collectent ou traitent des données personnelles, de vérifier que leurs activités et la technologie sous-jacente incluent les principes de sécurité des données et du respect de la vie privée.

Approche Dynamics 365 : Les services Dynamics 365 ont été développés en utilisant le concept Secure Development Lifecycle de Microsoft (développement sécurisé tout au long de la vie du produit), qui intègre des méthodologies de respect de la vie privée par conception et par défaut, en accord avec les politiques de respect de la vie privée de Microsoft. De plus, de nombreux services Dynamics 365 sont audités au moins une fois par an pour évaluer leur respect à diverses normes mondiales de sécurité des réseaux et de respect de la vie privée, comme la norme ISO/IEC 27018. En savoir plus sur le Centre de gestion de la confidentialité Microsoft Dynamics 365.

En savoir plus sur les normes de sécurité des réseaux et sur le respect de la vie privée

NORMES >

ISO/IEC 27018 >

Questions à étudier

Votre organisation répond-elle aujourd'hui à ces normes ?

En savoir plus sur le concept Secure Development Lifecycle de Microsoft

SITE WEB >

CHARTE DE CONFIDENTIALITÉ >

CENTRE DE GESTION DE >

Sécuriser les données personnelles par le chiffrement

Le GDPR demande aux responsables des traitements ou aux sous-traitants d'assurer une sécurité de très haut niveau. Le GDPR cite le chiffrement comme un outil qui répond potentiellement à cette exigence en garantissant un niveau de sécurité adapté au risque.

Approche Dynamics 365 : Dynamics 365 utilise des technologies comme le TDE (chiffrement transparent des données) pour chiffrer les données avec TLS (Transport Layer Security) afin de sécuriser les communications entre services. Pour Dynamics 365, le chiffrement au niveau de chaque champ est disponible dans Microsoft SQL Server pour un ensemble d'attributs par défaut qui contiennent des informations sensibles.

Les données personnelles que vous gérez sont-elles vraiment stockées chiffrées ?

TDE

TLS

CHIFFREMENT

Sécuriser les données personnelles en intégrant des contrôles de sécurité qui assurent la disponibilité, l'intégrité et la confidentialité des données personnelles

Le GDPR demande aux responsables des traitements d'appliquer des mesures organisationnelles et techniques appropriées pour sécuriser les données personnelles. Ces mesures doivent être appropriées pour le risque en question, en fonction du type d'activité et du coût des mesures.

Approche Dynamics 365 : Dynamics 365 propose plusieurs outils pour protéger les données en fonction des besoins de conformité et de sécurité de l'organisation. Plusieurs concepts de sécurité dans Dynamics 365 protègent l'intégrité des données et respectent la vie privée dans l'organisation. La sécurité basée sur des rôles vous permet de grouper des droits afin de limiter les tâches qu'un utilisateur peut réaliser. La sécurité basée sur les enregistrements vous permet de restreindre l'accès de certains enregistrements. La sécurité au niveau des champs vous permet de restreindre l'accès de certains champs tels que ceux contenant des informations liées à des personnes identifiables. Le chiffrement TDE permet de chiffrer au niveau des cellules. En savoir plus sur le Centre de gestion de la confidentialité Microsoft Dynamics 365.

L'approche actuelle de votre organisation pour sécuriser les données personnelles répond-elle à cette norme ?

CENTRE DE GESTION DE LA CONFIDENTIALITÉ

Détecter et répondre aux violations de données

Le GDPR demande aux responsables des traitements ou aux sous-traitants de mettre en œuvre des procédures et des technologies appropriées pour sécuriser les données personnelles et les protéger contre des violations de données. Si une violation de données personnelles se produit, dès lors que vous en êtes averti, vous devez avertir rapidement les régulateurs et il est possible que vous deviez aussi avertir les personnes concernées.

Approche Dynamics 365 : Dynamics 365 déploie des mesures de sécurité dans le but d'empêcher et de détecter des violations de données, comme des logiciels de détection d'intrusion et de prévention contre les attaques par déni de service distribué. Dynamics 365 répond aux incidents qui impliqueraient des données stockées dans les centres de données Microsoft, en suivant une procédure de gestion de la réponse à un incident de sécurité.

Votre organisation a-t-elle mis en place une procédure pour gérer les notifications d'une violation de données personnelles ?

En savoir plus sur les procédures de gestion des réponses à des incidents de sécurité

EN SAVOIR PLUS

Faciliter des tests réguliers des mesures de sécurité

Pour répondre aux conditions du GDPR qui visent à protéger les données personnelles, les responsables des traitements ou leurs sous-traitants doivent régulièrement tester et évaluer l'efficacité de leurs mesures organisationnelles et techniques pour sécuriser ces données.

Approche Dynamics 365 : Dynamics 365 fournit aux administrateurs des fonctionnalités d'audit qui facilitent l'identification des changements apportés aux données. Elles permettent aussi d'améliorer la sécurité pour protéger les données personnelles et détecter des violations de données. Microsoft mène aussi des contrôles et des tests continus des mesures de sécurité de Dynamics 365. Cela inclut une modélisation permanente des menaces, une révision du code, des tests de sécurité, des tests de pénétration des sites, ainsi qu'un contrôle et une journalisation centralisés de la sécurité.

L'approche de votre organisation pour tester la sécurité suit-elle ce standard ?

Signaler

Répondez à des demandes de données, signalez des violations de données et maintenez à jour la documentation.

Afin d'être en conformité avec le GDPR, vous devez assurer un audit de toutes les demandes, les activités de traitement, et leur résolution. Vous devez aussi suivre et enregistrer les flux de données personnelles qui entrent et sortent de l'UE, les fournisseurs de services, les transferts de données personnelles limités à certains pays et certains tiers avec des protections adéquates. Enfin, une Évaluation de l'impact de la protection des données (DPIA) doit être menée lors du traitement de données personnelles qui pourrait entraîner un risque élevé sur les droits et les libertés des personnes. Cette procédure interne évalue les risques potentiels et propose des solutions appropriées.

Assurer un audit permanent pour montrer la conformité au GDPR

Les responsables des traitements doivent enregistrer en permanence les activités de traitement sous leur responsabilité. Les enregistrements doivent contenir la nature de chaque demande, par exemple voir ou modifier des données personnelles, et leur résolution.

Approche Dynamics 365 : Dynamics 365 vous permet de suivre et d'enregistrer les modifications des données dans un environnement Dynamics 365. Les données et les opérations qui peuvent être auditées dans Dynamics 365 incluent la création, la modification et l'effacement d'enregistrements ; des changements apportés aux droits partagés des enregistrements ; l'ajout et la suppression d'utilisateurs ; l'affectation de rôles de sécurité ; et l'association d'utilisateurs à des équipes et des départements dans l'entreprise. Vous pouvez utiliser ces outils d'audit et de journalisation pour enregistrer la résolution des requêtes des personnes concernées, et pour enregistrer dans un journal toute opération de modification, d'effacement ou de transfert de données personnelles.

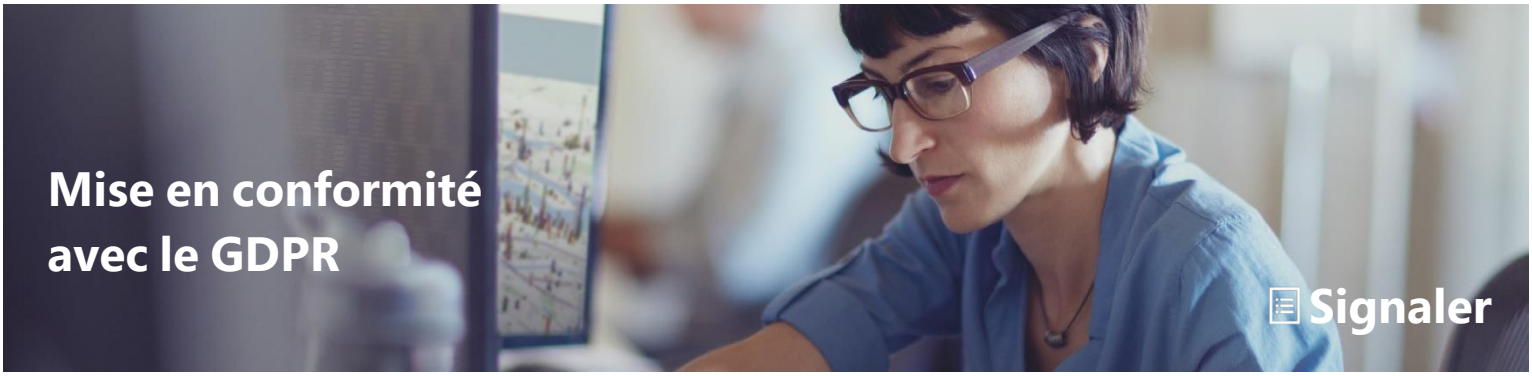
Suivre et enregistrer les flux de données personnelles de et vers l'UE

Le GDPR limite le transfert des données personnelles en dehors de l'UE aux pays qui appliquent des mesures de sécurité comparables ou appropriées.

Questions à étudier

Votre organisation enregistre-t-elle vraiment les activités de traitement ?

Avez-vous des mécanismes en place pour transférer des données personnelles en dehors de l'UE, comme des clauses contractuelles standards ou des règles d'entreprise contraignantes ?



Approche Dynamics 365 : Dynamics 365 réduit le besoin de transférer des données personnelles en dehors de l'UE en vous donnant le choix du lieu de stockage des données. Au cours de l'initialisation, vous pouvez choisir parmi les datacenters de plus de 30 régions dans le monde entier. De plus, Microsoft a pris des engagements contractuels dans Azure pour permettre un flux approprié de données personnelles à l'intérieur de l'écosystème Microsoft. Microsoft a mis en œuvre les Clauses du modèle de l'UE et a reçu la certification EU-US Privacy Shield.

En savoir plus sur les engagements contractuels de Microsoft

ENGAGEMENTS >

Suivre et enregistrer les flux de données personnelles avec des fournisseurs de service tiers

Le GDPR demande aux responsables des traitements de garder une trace des transferts de données personnelles avec des tiers, et demande à ces tiers de respecter les conditions du GDPR.

Approche Dynamics 365 : les clients Dynamics 365 qui jouent le rôle de responsables des traitements, sont responsables du suivi de la diffusion des données personnelles envers des tiers via leurs services personnalisées et des applications hébergées dans Dynamics 365. Microsoft répertorie les fournisseurs de service tiers qui ont accès aux données des clients. La Liste des sous-traitants Microsoft Online Services répertorie les sous-traitants de tous les services en ligne proposés dans la section Condition de traitement des données, du contrat Services en ligne.

À quelle fréquence votre organisation enregistre-t-elle les transferts de données personnelles des personnes concernées dans l'UE vers des fournisseurs de service tiers ?

FOURNISSEURS >

Faciliter l'évaluation de l'impact de la protection des données

Les responsables des traitements doivent mener une Évaluation de l'impact de la protection des données (DPIA) lorsqu'un traitement pourrait entraîner un risque élevé sur les droits et les libertés des personnes. C'est une procédure interne qui évalue, entre autres choses, des risques sur la vie privée et qui propose des corrections appropriées.

Approche Dynamics 365 : Dynamics 365 vous permet l'utilisation du journal d'audit Dynamics 365. Avec ce journal, vous pouvez suivre et enregistrer des activités de traitement dans l'écosystème Dynamics 365 et informer la procédure DPIA de votre organisation. Pour vous aider à trouver les informations d'utilisation de Dynamics 365, Microsoft fournit des informations détaillées sur la collecte et le traitement des données clients et sur les mesures de sécurité utilisées pour protéger ces données. Ces informations, accessibles via le Centre Microsoft de gestion de la confidentialité, inclut les données collectées et traitées par Microsoft, comment et où Microsoft envoie les données des clients, les sous-traitants qui ont accès aux données du client, des détails sur les mesures de sécurité de Dynamics 365 et des détails sur la procédure de révision de la confidentialité chez Microsoft.

Pour obtenir des informations supplémentaires, visitez Microsoft.com/GDPR. En raison de l'importance des modifications à prévoir, vous ne devriez pas attendre pour vous préparer. Passez en revue dès à présent vos pratiques de gestion des données et notamment, des données personnelles.

Votre organisation gère-t-elle vraiment des DPIA ?

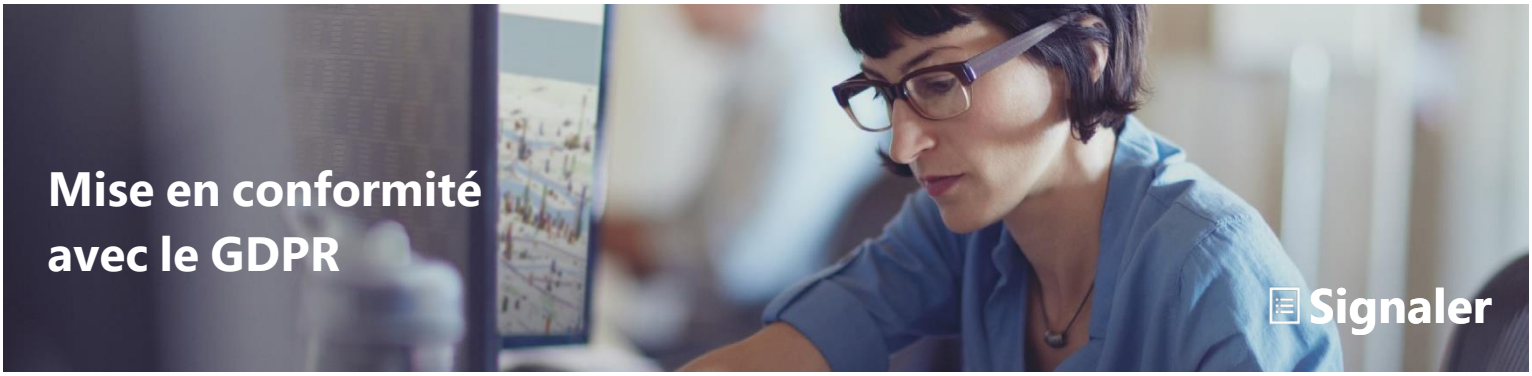
En savoir plus

Données collectées et traitées par Microsoft

EN SAVOIR PLUS >

Comment et où Microsoft envoie les données des clients

EN SAVOIR PLUS >



Ce livre blanc montre comment Dynamics 365 prend en charge votre mise en conformité avec le GDPR, ainsi que les approches, les pratiques recommandées et les techniques pour vous aider à vous mettre en conformité.

Liens additionnels

En savoir plus sur le GDPR à l'adresse Microsoft.com/GDPR

SITE WEB >

Offres et tarifs de Dynamics 365

TARIFS >

En savoir plus sur les sous-traitants qui accèdent aux données des clients

EN SAVOIR PLUS >

En savoir plus sur les mesures de sécurité de Dynamics 365

EN SAVOIR PLUS >

En savoir plus sur la procédure de révision de la confidentialité chez Microsoft

EN SAVOIR PLUS >

Comment obtenir Dynamics

Démarrez avec Dynamics 365 dès aujourd'hui !

- Options pour un ou plusieurs produits
- Choix pour tous types d'utilisateurs
- Éditions pour des entreprises de toutes tailles

DÉMARRER >