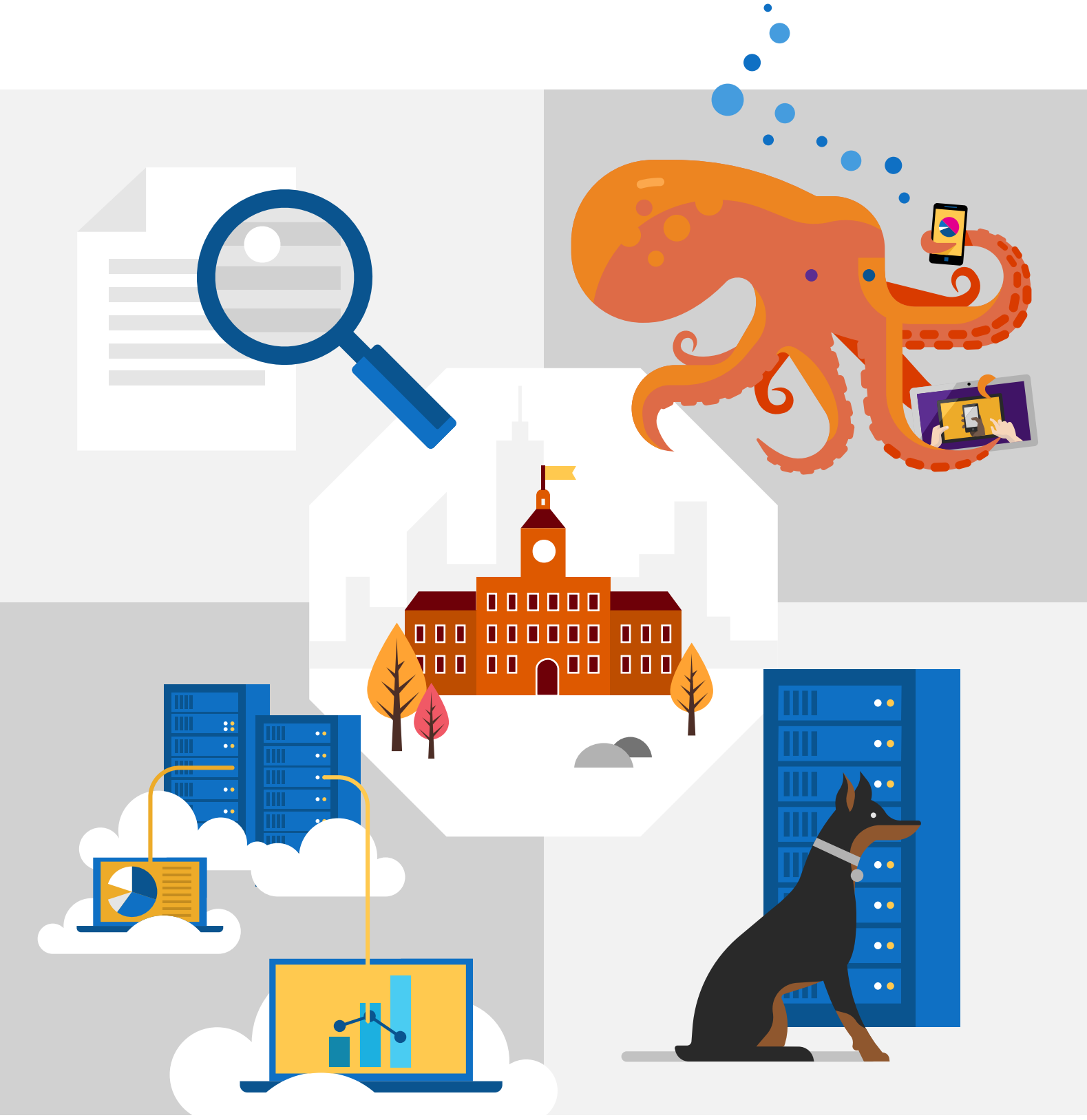


Protection des données : le RGPD dans l'éducation

Guide de démarrage pour
les établissements scolaires

Microsoft

À propos de ce guide

Ce guide a pour but de faciliter votre mise en conformité avec le Règlement Général sur la Protection des Données personnelles (RGPD) à l'aide d'exemples concrets et de listes de tâches. Il n'est pas exhaustif, mais donne un aperçu des procédures et facteurs à prendre en compte à partir du 25 mai 2018, date de l'entrée en vigueur du RGPD.

Le RGDP s'applique aux établissements ayant une présence physique dans l'Union Européenne et aux organisations qui fournissent des biens et services à des citoyens de l'UE ou qui collectent et analysent des données relatives à des résidents de l'UE.

L'éducation, une question de données

À chaque début d'année scolaire, les nouveaux élèves et étudiants génèrent des quantités phénoménales de données dans les écoles et universités.

De telles données sont indispensables au fonctionnement des écoles et universités. Il s'agit donc de mettre en place des procédures claires et bien documentées pour chaque dossier traité.

Ces procédures doivent en outre rester en vigueur même après que l'étudiant ait quitté votre établissement. Au départ de ce dernier, les bases de données, les dossiers, voire les échanges d'e-mail nécessiteront des politiques documentées en matière de protection, de rétention et de traitement.

Définition du parcours des données

Les informations créées et traitées dans des établissements scolaires ont diverses finalités.

Il y a tout d'abord le programme scolaire, les connaissances que les enseignants partagent avec les élèves et les étudiants, étoffées par les idées que les étudiants génèrent au il de leur apprentissage.

Il y a aussi un second ensemble de données : les informations collectées par des organisations sur les enseignants, les élèves et les étudiants, ainsi que les performances de l'école. Ajoutez à cela les informations collectées au cours de procédures administratives – parents, in irmières scolaires, directeurs, conseillers et agences externes – et vous obtiendrez un très grand nombre de données circulant au sein de l'organisation et qui sont en grande partie des données personnelles.

Chaque administrateur sait que ce second jeu de données est tout aussi crucial pour un établissement d'enseignement que sa mission éducative. Ces datas font partie du parcours de conformité RGPD que les étudiants, enseignants et parents suivent en accédant à des informations et en partageant celles-ci grâce aux outils d'apprentissage et de communications fournis par les écoles et universités.

Que faire de toutes ces données ?

En tant que responsable du traitement des données, vous respectez déjà la législation existante qui préconise une manipulation et un traitement scrupuleux des données que vous détenez et gérez. Même s'il existe des préconisations supplémentaires avec le RGPD relatives aux modalités et raisons de la divulgation, aux organisations avec lesquelles vous devez partager des données partielles –ex. organismes de réglementation en plus de tiers, comme les assureurs – à leur traitement et à leur analyse, vous avez très probablement déjà mis en place diverses politiques de protection des données et de respect de la vie privée.

Présentation du RGPD

À compter du 25 mai 2018, les organisations, y compris celles se trouvant en dehors de l'Union européenne (UE), seront responsables du traitement des données qu'elles collectent, en vertu de la nouvelle réglementation de l'UE, le Règlement Général de la Protection des Données personnelles (RGPD).

Ce règlement a pour objet de protéger les données personnelles de tous les citoyens de l'UE et d'harmoniser toutes les lois relatives à la protection des données personnelles en Europe.

Le RGPD affectera les données en votre possession, la façon dont vous les utilisez, leur lieu de stockage et la durée possible de leur stockage.

Pourquoi le RGPD est-il important ?

Un cursus éducati peut refléter le parcours d'apprentissage d'un étudiant, avec des étapes enregistrées et évaluées à chaque fois. Les données pourront rester identiques pendant des années, tandis que d'autres changeront rapidement au fur et à mesure de l'évolution des étudiants et du personnel au sein de l'établissement.

Le RGPD crée un cadre légal européen uniforme qui confère aux résidents européens des droits sur ces données.

Les changements majeurs qui affectent l'éducation sont les suivants :

Vie privée

Les personnes ont le droit :

- d'accéder à leurs données personnelles
- de corriger les erreurs dans leurs données personnelles
- de supprimer leurs données personnelles
- de s'opposer au traitement de leurs données personnelles
- d'exporter leurs propres données personnelles

Contrôles et notifications

Vous devrez :

- protéger les données personnelles avec des mesures de sécurité appropriées
- signaler des violations de données personnelles aux autorités
- documenter votre traitement de données personnelles
- tenir des registres détaillés du traitement de données et des autorisations*

Politique transparente

Vous serez censé(e) :

- notifier clairement une collecte de données
- exposer les objectifs de traitement et cas d'utilisation
- définir des politiques de conservation et de suppression de données
- exposer la manière dont les clients peuvent exercer leurs droits dans le cadre du RGPD

IT et formation

Les établissements d'enseignement devront :

- former leur personnel et leurs employés au traitement de données personnelles – ex. administrateurs ou personnel IT
- auditer et actualiser les politiques de données relatives aux élèves et aux étudiants, au personnel et aux prestataires
- Engager un Responsable de la protection des données (si nécessaire)
- créer et gérer des contrats de fournisseurs conformes, y compris tous les fournisseurs et enseignants

***Le RGPD inclut une protection spécifique des enfants. Il suppose de manière générale que le consentement d'un enfant doit être « explicite ». Le RGPD fixe l'âge de consentement à 16 ans concernant les contenus en ligne. Des États membres de l'UE peuvent toutefois fixer individuellement l'âge de consentement entre 13 et 16 ans.**

En quoi le RGPD vous concerne-t-il ?

Comment concilier ce nouveau règlement avec le fait, qu'au quotidien, diverses personnes d'un établissement doivent accéder aux données ?

Le RGPD prescrit la manière de gérer et de protéger ces données en mettant en place des politiques et pratiques cohérentes. Il vous appartient de créer un plan de mise en conformité au RGPD viable pour votre établissement.

Extension des droits à la protection de la vie privée

Le RGPD renforce la protection des données de particuliers, élèves et étudiants y compris, au sein de l'UE en leur garantissant le droit :

- d'accéder à leurs données et de corriger les erreurs
- de supprimer leurs données
- de s'opposer au traitement de leurs données
- de déplacer leurs données

Obligation accrue de documenter les procédures et de protéger les données

Les établissements d'enseignement qui traitent des données personnelles devront fournir la preuve claire de leur conformité.

Signalement obligatoire de toute violation de données

Les établissements d'enseignement sont tenus de signaler toute violation des données dans un délai de 72 heures.

Sanctions graves en cas de non-conformité

Les établissements d'enseignement s'exposent à des amendes potentielles s'ils négligent de réagir. Afin d'être conformes, ils devront envisager plusieurs mesures de protection des données personnelles et manipuler celles-ci avec prudence.

Par quoi commencer ? Cartographie de la conformité au RGPD

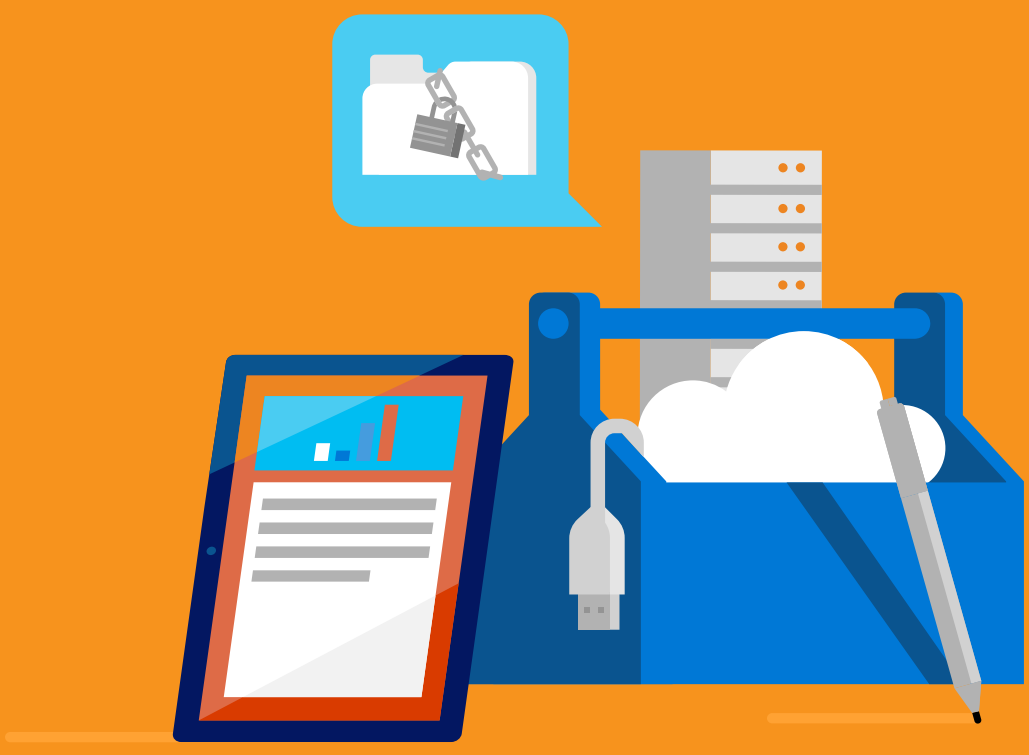
Le RGPD a un impact significatif sur votre établissement. Il exigera l'actualisation de votre politique de protection de la vie privée, la mise en œuvre ou le renforcement de vos contrôles de la protection des données et de vos procédures de signalement des violations, le déploiement de politiques très transparentes et l'investissement continu dans l'IT et la formation.

Le Cloud Microsoft peut faciliter votre mise en conformité avec le RGPD grâce à un éventail complet d'offres de conformité. Le Cloud Microsoft vous propose la plupart des ressources nécessaires pour répondre aux exigences du RGPD.

Nous avons développé une procédure pour mettre en œuvre le RGPD en vous concentrant sur quatre étapes-clés :

- **Découvrir.** Identifiez les données personnelles en votre possession et leur lieu de stockage.
- **Gérer.** Gérez le mode d'utilisation et d'accès des données personnelles.
- **Protéger.** Mettez en place des contrôles de sécurité pour prévenir et détecter des vulnérabilités et violations de données et y réagir.
- **Signaler.** Conservez la documentation nécessaire et gérez les demandes de données et signalements de violations.

Les outils et ressources de Microsoft peuvent vous aider à chaque étape de mise en conformité avec le RGPD.



Découvrir

Gérer

Signaler

Protéger

Découvrir

Identifiez les données personnelles en votre possession et leur lieu de stockage.

Découvrez les données en votre possession

Les données personnelles sont souvent stockées dans divers endroits, y compris dans des e-mails, documents, bases de données, supports amovibles, métadonnées, historiques et copies de sauvegarde.

La première étape consiste à identifier l'endroit où les données personnelles sont collectées et stockées.

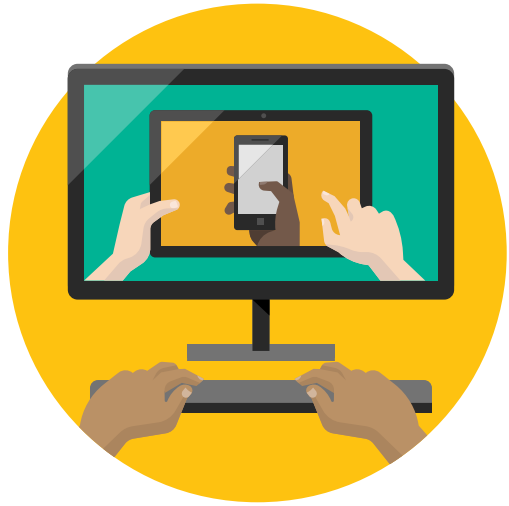
Données existantes

Défi

Vous devez non seulement stocker et sécuriser des données conformément au RGPD, mais aussi documenter votre traitement de données personnelles ex. 1. autorisation, 2. contrat, 3. aspect légal, 4. santé, 5. cause commune, 6. cause légitime.

À faire

- identifier les données personnelles existantes collectées et stockées.
- découvrir les lieux de stockage de ces données. Inclure des fournisseurs cloud et hôtes tiers comme les sites Web et centres de services partagés. Ne pas oublier les données analogiques comme les fichiers se trouvant dans des armoires de classement.
- organiser et étiqueter les données existantes en fonction de leur confidentialité, de leur utilisation, de leurs propriétaires, administrateurs et utilisateurs.
- documenter les raisons du traitement RGPD.
- vérifier l'autorisation de traitement et la renouveler le cas échéant.



Appareils existants et sites

Défi

Les données personnelles sont souvent stockées et accessibles sur un grand nombre d'appareils pouvant inclure des serveurs, ordinateurs de bureau, ordinateurs portables, tablettes, smartphones, ordinateurs domestiques et environnements cloud gérés et non-gérés. Les appareils personnels et mobiles rendent la découverte de données difficile.

À faire

- dresser un inventaire et répertorier tous les appareils susceptibles de contenir des données personnelles.
- vérifier les appareils personnels et portables qui n'appartiennent pas à l'établissement.

Exigences du RGPD

Le RGPD exige que les organisations identifient les données existantes et leur lieu de stockage.

Après avoir dressé l'inventaire de toutes les données, y compris des sites, des appareils et des utilisateurs, vous pourrez configurer des systèmes pour la collecte de nouvelles données entrantes.

Utilisateurs existants

Défi

Le RGPD définit strictement les personnes habilitées à traiter des données personnelles et les modalités d'un tel traitement (comment et quand). Avant de partager des données personnelles, assurez-vous que les personnes y ayant accès ont le droit de les consulter, tant à l'intérieur qu'à l'extérieur de l'école.

À faire

- identifier et répertorier tous les utilisateurs, y compris les étudiants, le personnel et tous les prestataires susceptibles d'accéder à des données.

Sous-traitants existants

Défi

Les données personnelles ne doivent être divulguées qu'aux personnes autorisées et n'être accessibles que par celles-ci. Il s'agit de personnes se trouvant tant à l'intérieur qu'à l'extérieur de l'organisation, par exemple tous les prestataires – y compris les services de restauration, de nettoyage et les assistants externes – qui travaillent avec votre établissement.

Il vous appartient de vérifier si les personnes autorisées à accéder aux données – appelées processeurs dans le RGPD – respectent la législation. Autrement dit, si elles stockent des données de manière sécurisée, n'utilisent celles-ci qu'aux fins définies par vous et les détruisent lorsqu'elles n'en ont plus besoin.

À faire

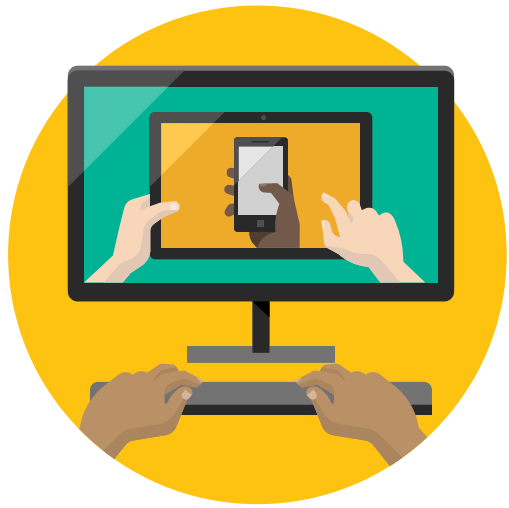
- identifier et répertorier tous les sous-traitants dans le répertoire d'utilisateurs.
- vérifier leur conformité au RGPD.
- signer un contrat de conformité au RGPD.
- vérifier la possibilité d'accès centralisé aux données alors que celles-ci se trouvent encore sur place.

Gérer

Gérez les modalités d'utilisation et d'accès aux données personnelles

Gestion de données personnelles

La première étape de la gestion de données personnelles consiste à définir la raison première de leur collecte. Demandez-vous dans quelle mesure cela facilite la fourniture de services éducatifs. Réfléchissez à la façon dont il faudrait les collecter, à leur lieu de stockage, aux entités prenant cette procédure en charge, aux personnes qui doivent y accéder et à la manière dont vous autorisez des changements et suppressions.



Gestion de données nouvelles

Défi

Le RGPD vous autorise à utiliser des données nécessaires à l'exécution de votre mission. Si cette dernière est clairement définie, le besoin de traiter les données personnelles augmentera.

Lors de l'inscription d'étudiants, vous devrez faire preuve de transparence quant aux données personnelles collectées. Vous devrez en particulier savoir à quelles fins vous avez besoin de ces données, combien de temps vous les garderez, où vous les stockerez et comment vous et des tiers y accéderez. Vous devrez, le cas échéant, demander, obtenir et conserver à titre de preuve l'autorisation de traiter les données.

Les élèves et les étudiants mineurs auront besoin de l'autorisation de leurs parents. Lorsque vous engagerez du personnel, vous devrez l'informer clairement sur le mode de traitement de données personnelles.

À faire

- définir clairement votre mission.
- répertorier les personnes concernées.
- déterminer les données personnelles requises.
- automatiser la collecte de données et vous montrer responsable.
- expliquer les clauses RGPD de contrats avec le partenaire RH et vérifier les procédures d'autorisation et de renouvellement, le cas échéant.

Gestion d'appareils

Défi

Dans un contexte éducatif, les appareils sont multiples et répartis entre de nombreux utilisateurs : ordinateurs personnels d'enseignants, smartphones et tablettes d'étudiants, ordinateurs de salle de classe, appareils personnels, applications privées, applications cloud et autre non-surveillées, appareils de sous-traitants, clés USB et dossiers sur papier dans des armoires de classement.

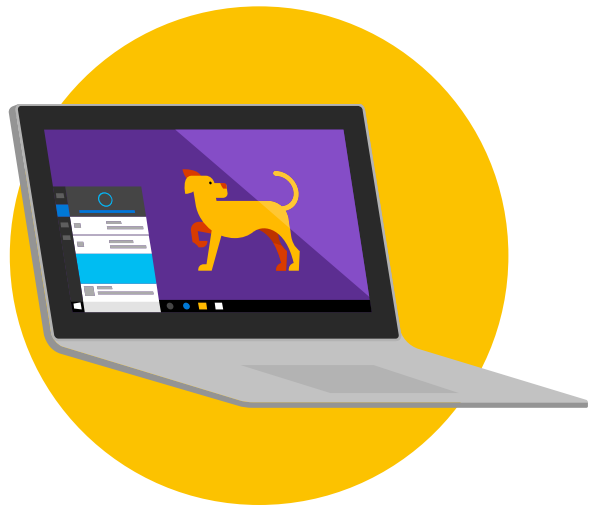
Pour répondre aux exigences strictes du RGPD en matière de protection des données personnelles, vous devez gérer les appareils – ainsi que le personnel enseignant, les étudiants et prestataires – de manière cohérente.

À faire

- élaborer une politique relative à l'utilisation d'appareils.
- éduquer le personnel et les étudiants et les sensibiliser au RGPD.
- auditer et enregistrer des événements.

Exigences du RGPD

Le RGPD régit les modalités d'utilisation et d'accès des données personnelles.



Gestion des utilisateurs

Défi

Tandis que la procédure de découverte vous donne une idée de votre base de données d'utilisateurs, la gestion vous aide à organiser les utilisateurs en listes intelligentes qui vous permettent de définir des autorisations, sécuriser une politique d'authentification et suivre les accès.

Lorsqu'ils quittent votre établissement, les utilisateurs ne doivent plus avoir accès à toutes les ressources scolaires afin d'éviter des fuites potentielles.

À faire

- organiser les utilisateurs en groupes de sécurité.
- définir des autorisations et politiques.
- mettre des politiques en place.
- former les élèves et les étudiants, le personnel et les prestataires à l'utilisation correcte de données.

Gestion de votre site web

Défi

Les activités en ligne représentent une part cruciale de la promotion visant à attirer du personnel et des étudiants. Il vous appartient de garantir la sécurité sur les plates-formes en ligne que vous utilisez.

À faire

- auditer les données collectées automatiquement par votre site web.
- répertorier les cookies prioritaires et tiers.
- vérifier la sécurité de bout en bout de formulaires en ligne.
- vérifier la conformité des procédures d'autorisation au RGPD.
- créer une déclaration de confidentialité documentant :
  - le type d'informations collectées
  - la personne qui les collecte
  - leurs modalités de collecte
  - la raison de leur collecte
  - l'utilisation qui en sera faite
  - le destinataire avec qui les informations seront partagées
  - l'impact sur les personnes concernées
  - si l'utilisation prévue est susceptible de donner lieu à des objections ou plaintes

Protéger

Établissez des contrôles de sécurité pour prévenir, détecter des vulnérabilités & violations de données et réagir.

Protection des utilisateurs, données et appareils

La sécurité est l'une des priorités clés de notre monde informatisé.

La protection physique, la sécurité des réseaux, la sécurité de stockage, la sécurité informatique, la gestion des identités, le contrôle des accès, le chiffrement et l'atténuation des risques font partie des exigences du RGPD. Examinez votre méthode de contrôle des systèmes, identifiez les violations, calculez l'impact de violations, empêchez-les et remédiez-y.

Données

Défi

Le RGPD n'est pas une destination, mais un cheminement continu.
Il exige que vous soyez responsable en permanence, réagissiez rapidement si nécessaire et protégiez les données personnelles circulant au sein de votre établissement.

À faire

- chiffrer les données et e-mails.
- protéger les données sur les appareils (MAM).
- stocker les données de manière sécurisée.
- ajouter des droits à des fichiers individuels et e-mails.
- surveiller les intrusions, infections, vols et comportements anormaux.

Appareils, sites et applications

Défi

Les appareils et applications concernent à peu près tous les aspects de vos données.
Ils peuvent faire partie de votre réseau local (RL), d'appareils portables, d'appareils localisés ailleurs, par exemple à la maison ou sur le campus, et d'appareils et d'applications dans le cloud. Tous les appareils et applications nécessitent une attention particulière.

À faire

- protéger le RL avec un logiciel antivirus, un firewall et une protection physique.
- chiffrer les appareils, disques et clés USB.
- former les étudiants et le personnel aux meilleures pratiques concernant les ordinateurs domestiques.

Exigences du RGPD

Le RGPD définit les règles pour la mise en place de contrôles de sécurité dans le but de prévenir et de détecter des vulnérabilités et violations de données et d'y réagir.

Utilisateurs

Défi

Après avoir défini et organisé les utilisateurs en groupes de sécurité avec des autorisations et politiques spécifiques, vous pouvez ajouter des mesures de protection – contrôle des accès et gestion des identités – pour être conforme au RGPD.

À faire

- réviser la politique de mots de passe et les options d'authentification.
- éduquer et sensibiliser.

Tests

Défi

Après avoir mis en place les mesures techniques et organisationnelles pour protéger les données personnelles, vous devez les tester régulièrement et évaluer leur efficacité pour vous assurer qu'elles sont adéquates et appropriées.

À faire

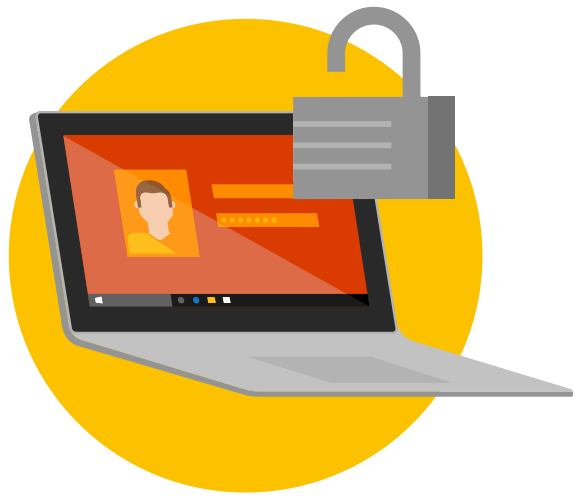
- faciliter des tests réguliers.
- évaluer l'efficacité des mesures de sécurité.

Signaler

Répondez aux demandes de données, signalez des violations de données et conserver la documentation requise.

Rapports d'audits et de violations de données

La responsabilité est l'un des principes clés du RGPD. Vous devrez créer des pistes d'audit claires concernant le traitement, les classifications et les tiers ayant accès à des données personnelles, y compris des mesures de sécurité organisationnelles et techniques et les durées de conservation des données. Il pourra vous être demandé de procéder à des Analyses d'Impact sur la Protection des Données (DPIA). Dans le cadre d'une DPIA, les organisations doivent identifier et analyser l'impact d'une activité de traitement proposée sur la protection de données personnelles.



Pistes d'audit

Défi

Dans le cadre du RGPD, vous devez assumer la sauvegarde et le traitement approprié de données personnelles. Vos registres doivent mentionner la nature de chaque demande émanant d'une personne concernée – par exemple pour visualiser ou rectifier des données personnelles – et la résolution qui a suivi.

À faire

- conserver les registres de demandes de personnes concernées afin de prouver la conformité aux exigences du RGPD.
- suivre et enregistrer les flux entrants et sortants de données personnelles dans l'UE.
- suivre et enregistrer les données envoyées à des fournisseurs de services tiers, ex. prestataires IT ou services éducatifs.
- actualiser les pistes d'audit pour prouver la conformité au RGPD.
- suivre et enregistrer les flux de données personnelles à des fournisseurs de services tiers.
- faciliter les DPIA.

Violations de données

Défi

Les organisations devront signaler dans les 72 heures toute violation identifiée aux autorités compétentes.

À faire

- activer les journaux et rapports.
- réagir dans le délai requis.
- tenir un journal séparé des changements de données personnelles en cas de catastrophe et de restauration de sauvegarde.

Exigences du RGPD

Les organisations devront signaler dans les 72 heures toute violation identifiée aux autorités compétentes.

Conclusion

La confiance est le pilier autour duquel s'articule la mission de Microsoft consistant à permettre à chaque personne et à chaque organisation de réaliser leurs ambitions. Celle-ci est cruciale dans les établissements scolaires qui préparent la prochaine génération d'étudiants à trouver et réaliser leurs objectifs au sein de la société.

Microsoft s'engage à appliquer ses principes de confiance cloud via la sécurité, le respect de la vie privée, la transparence et la conformité. Le RGPD prenant effet le 25 mai 2018, la gamme étendue de services cloud de Microsoft permet
de respecter la vie privée de nos clients dans le secteur de l'éducation et garantir que nous vous aidons à répondre à vos obligations en tant que responsable du traitement des données.

L'offre Office 365 A1, incluant la productivité cloud de Microsoft, est gratuite pour les clients du secteur de l'éducation. Elle fournit les outils essentiels de protection des données permettant de se conformer au RGPD, facilitant l'eDiscovery, la gestion des droits, la prévention de perte de données, le chiffrement, l'archivage avancé d'e-mails et la durée légale de conservation. Les clients qui requièrent une analyse détaillée des risques, un chiffrement et un contrôle de données, peuvent envisager d'acquérir la version payante d'Office 365 A3 ou A5 pour répondre à leurs besoins spécifiques en matière de conormité au GDPR.

Les clients à la recherche de solutions qui gèrent l'archivage, la gouvernance et la découverte de données pour leur secteur IT peuvent utiliser Microsoft 365 Education qui offre une expérience simple et sécurisée pour gérer des utilisateurs, données et appareils à partir d'un seul tableau de bord qui protège les identités, applications, données et appareils avec une sécurité intelligente améliorée par l'apprentissage machine.

Commencez dès aujourd'hui à utiliser l'outil d'évaluation du RGPD sur le Trust Center Microsoft afin de connaître votre niveau global de préparation. Et si vous êtes déjà un client Microsoft Cloud, utilisez Compliance Manager pour avoir une vue d'ensemble sur votre protection des données et de votre niveau de conformité pour Office 365, Dynamics 365 et Azure.

Outils et liens associés

Nous avons dressé la liste suivante d'outils afin de vous aider dans votre parcours RGPD.

Découvrir

- **Office 365 Advanced eDiscovery** ou **Content Search** vous aidera à chercher des informations existantes.
- **Office 365 data labelling** vous permettra de classer des données dans votre organisation aux fins de gouvernance.
- **SharePoint Lists** est un outil flexible qui vous aide à organiser et étiqueter des données.
- **User Account Management** dans Office 365 vous aide à organiser les utilisateurs.
- **Microsoft Intune for Education** vous aide à répertorier et gérer divers appareils.
- **System Center** est la solution idéale pour répertorier et gérer des serveurs avec divers SE et solutions cloud hébergées.
- **Azure Search** vous aidera à ajouter une fonctionnalité de recherche à votre environnement actuel.
- **Azure Data Catalog** enregistre, découvre, comprend et consomme des sources de données.
- **Cloud Discovery** analyse vos journaux de trafic par rapport au catalogue Cloud App Security avec plus de 15 000 applications cloud classées et notées selon plus de 60 facteurs de risques, afin de vous offrir une visibilité constante de l'utilisation du cloud, du Shadow IT et du risque présenté par le Shadow IT pour votre organisation.
- **Advanced Data Governance** (ADG) vous aide à identifier, classer et gérer automatiquement des données personnelles et sensibles, ainsi qu'à appliquer des politiques de conservation et de suppression.

Gérer

- **Security Groups dans Office 365** permet de définir un seul jeu d'autorisations dans les applications Office 365.
- **Outlook Smart Attachments** empêche les données de quitter votre établissement.
- **Office 365 Mail Tips** permet d'éviter des erreurs courantes.
- **Office 365 Data Loss Prevention** empêche les données de quitter votre établissement.
- La création de **Flux** automatisés entre des applications optimisera et sécurisera les flux de données.
- **Intune for Education** vous aide à gérer les politiques, applications, configurations pour vos appareils de salles de classe.
- **Azure AD** (Azure Active Directory) est le service de gestion de répertoire et d'identité basé sur le cloud de Microsoft.
- **PowerApps** vous aide à créer des applications mobiles en un tour de main et à alimenter directement des bases de données.
- Appliquez des **étiquettes** à des données personnelles et gérez la **gouvernance de données** dans Office 365.
- **Azure Information Protection** contrôle et aide à sécuriser les e-mails, documents et données sensibles que vous partagez en dehors de votre société.
- L'intégration de **Microsoft Forms** (Office 365) peut sécuriser l'entrée de données via des formulaires en ligne et permet d'émettre des demandes d'autorisation conformes au RGPD.
- **Office 365 Teams** permet à des établissements de centraliser et de coordonner toutes les communications requises pour la politique RGPD.

Signaler

- Le **Microsoft Trust Center** est la source idéale pour vérifier des informations sur le RGPD et la conformité.
- **Microsoft Compliance Manager** vous aide à procéder à des évaluations de risques et simplifie votre procédure de conformité en recommandant des actions, réunissant des preuves et vous préparant à un audit.
- **Azure Auditing and Logging** vous fournit un enregistrement électronique d'activités suspectes et vous aide à détecter des modèles susceptibles d'indiquer une tentative de pénétration ou une infiltration externe réussie du réseau, ainsi que des attaques internes.
- **Securescore.office.com** est un outil d'analyse de la sécurité qui vous aide à comprendre les mesures que vous avez prises pour réduire le risque pour vos données dans Office 365 et montrera d'autres actions à mener à cet effet. Il est la source idéale de connaissance sur l'audit, la connexion et de nombreuses autres fonctions de sécurité d'Office 365.
- **Unified Audit log** donne un aperçu des données qui ont été communiquées à des tiers.

Protéger

- **Office 365 (A3) Data Loss Prevention** permet de créer des règles pour empêcher les types souhaités d'informations de quitter l'établissement.
- **Azure Information Protection** contrôle et aide à sécuriser les e-mails, documents et données sensibles que vous partagez en dehors de votre société. De la classification facile aux étiquettes et autorisations intégrées, améliorez toujours la protection de vos données avec Azure Information Protection – où qu'elles soient stockées et quel que soit leur destinataire.
- **Customer Lockbox** permet aux contrôleurs de prouver que des procédures explicites sont en place pour l'accès au contenu de clients pendant des opérations de service.
- **AppLocker** aide les administrateurs à créer et déployer des politiques de contrôle des applications, en restreignant les accès par des utilisateurs non-autorisés à des applications qui compromettent les données personnelles.
- **Microsoft Advanced Threat Analytics (ATA)** est une plate-forme sur place qui vous aide à protéger votre école contre divers types de cyberattaques ciblées et avancées et des menaces internes.
- **Office 365 Threat intelligence.**
- **Intune for Education** est une solution simple et puissante pour déployer des politiques, applications et configurations de sécurité pour vos appareils de salles de classe.
- **Windows Defender Advanced Threat Protection**, disponible dans Windows 10 Education, est un service de sécurité qui permet aux entreprises de détecter, d'examiner des menaces avancées sur leurs réseaux et d'y réagir.
- **Azure Backup et Azure Disaster Recovery** améliore le degré de disponibilité des données.
- **BitLocker Drive Encryption** est une fonctionnalité de protection des données qui s'intègre dans le système d'exploitation et traite les menaces de vols de données et d'exposition à des pertes, vols ou déclassements inappropriés d'ordinateurs.
- Utilisez **Multi Factor Authentication** dans Office 365 et Windows avec Windows Hello.

Remarque : il ne s'agit pas d'une liste exhaustive d'outils et services Microsoft disponibles pour faciliter les quatre étapes-clés. Si vous voulez en savoir plus sur la façon dont tous les produits et services cloud de Microsoft Cloud peuvent aider les clients à remplir leurs obligations RGPD, téléchargez l'ouvrage numérique "Accélérez votre conformité au RGPD avec le Microsoft Cloud".

Cet ouvrage est un commentaire général sur le RGPD tel que Microsoft l'interprète à compter de sa date de publication. Nous avons longuement étudié le RGPD et estimons avoir analysé sérieusement son contenu et sa portée. L'application du RGPD est toutefois liée aux situations factuelles et spécifiques d'une organisation et les aspects et interprétations du RGPD ne sont pas définis en détail.

Cet ouvrage électronique n'est par conséquent fourni qu'à titre informatif et ne doit pas être invoqué comme un conseil juridique ou pour déterminer la manière dont le RGPD pourrait s'appliquer à vous et à votre organisation. Nous vous suggérons de contacter un conseiller juridique qualifié pour discuter du RGPD, de façon dont il s'applique spécifiquement à votre organisation et du meilleur moyen de garantir votre conformité à celui-ci.

MICROSOFT N'ÉMET AUCUNE GARANTIE, EXPLICITE, IMPLICITE OU LÉGALE QUANT AUX INFORMATIONS CONTENUES DANS CET OUVRAGE ÉLECTRONIQUE. Cet ouvrage électronique est fourni « en l'état ». Les informations et avis exprimés dans celui-ci, y compris des URL et autres références à des sites Web sont susceptibles de modifications sans préavis.

Ce document ne vous confère aucun droit légal sur une propriété intellectuelle dans des produits Microsoft. Vous n'avez le droit de copier et d'utiliser cet ouvrage électronique qu'à des fins de référence.

Publication en mars 2018 Version 1.0

© 2018 Microsoft. Tous droits réservés.