Se conformer au RGPD

En quoi Act! CRM peut-il aider les entreprises à se conformer au Règlement général sur la protection des données ?

Qu'est-ce que le RGPD ?

Le Règlement général sur la protection des données (RGPD) s'applique à l'utilisation et au stockage des informations personnelles des citoyens européens. Chaque organisation dans le monde entier doit s'y conformer si elle souhaite se conformer au droit européen. Le RGPD a un impact à l'échelle de l'organisation et ce document explique comment Act! peut aider une organisation à s'y conformer.

Le RGPD est entré en vigueur le 25 mai 2018. Le RGPD veille à ce que toutes les entreprises utilisant les informations personnelles des résidents européens agissent dans le respect de la vie privée et des autres normes énoncées dans le RGPD. Certains des concepts et des principes réglementaires déjà existants en matière de confidentialité des données – ayant trait, par exemple, aux renseignements personnels, à la protection des renseignements médicaux et autres renseignements très personnels, ainsi qu'aux demandes d'accès par sujet - n'ont été que légèrement modifiés ou améliorés par le RGPD. Le RGPD a cependant introduit de nouvelles réglementations et exigences – avec notamment des droits personnels renforcés, comme la possibilité d'arrêter le traitement automatisé, ainsi que des principes de responsabilité plus stricts.

Le RGPD et Act! CRM

Les organisations qui communiquent ouvertement sur la façon dont elles travaillent dans le cadre du RGPD sont susceptibles d'avoir la confiance des prospects et des clients, leur conférant ainsi un net avantage par rapport à leurs concurrents. Inversement, le non-respect du RGPD peut entraîner des amendes monétaires et une perte de réputation. Par conséquent, il est essentiel que les entreprises adoptent une approche continue pour revoir et mettre à jour leurs processus et politiques commerciales, afin d'être et de demeurer conformes au RGPD.

En tant que solution hautement flexible et personnalisable, Act! CRM offre une grande variété de fonctionnalités qui peuvent aider les utilisateurs à gérer efficacement le traitement de leurs données ainsi que leur confidentialité et leur sécurité. S'il est correctement utilisé et adopté au sein de votre entreprise, Act! CRM peut être un outil extrêmement efficace pour se conformer au RGPD, dans le cadre d'un projet plus large de conformité à la réglementation du RGPD. Ce document vous aidera à comprendre certains des aspects clés du RGPD et vous fournit des informations sur l'aide que peut vous apporter l'utilisation d'Act! CRM dans votre conformité.

Table des matières

9 domaines pour lesquels Act! CRM peut aider avec le RGPD :

1. Définir les données personnelles 3
2. Contrôleurs et processeurs de données 3
3. Champ d'application territorial 3
4. Principes de protection des données 4
5. Base légale pour le traitement 7
6. Droits individuels 8
7. Responsabilité et gouvernance 14
8. Désignation d'un délégué à la protection des données .. 16
9. Sécurité des données personnelles 16

Avertissement : Ce document a été rédigé par Act! International Limited, une société britannique. Le bureau du Commissaire à l'information du Royaume-Uni (ICO) est l'autorité de surveillance principale pour Act! LLC et ce guide a été rédigé en référence au guide RGPD de l'ICO pour les organisations basées au Royaume-Uni. Comme le RGPD est une loi harmonisée à travers l'Union Européenne, nous pensons que ce guide devrait être applicable à toutes les organisations basées dans l'UE. Cependant, les informations contenues dans ce guide ne constituent pas un avis juridique et ne couvrent pas toutes les façons dont le RGPD peut impacter votre entreprise. Nous vous recommandons de collaborer avec un spécialiste juridique pour vous aider à évaluer pleinement les exigences de votre entreprise en ce qui a trait au RGPD et pour assurer votre conformité dans votre pays. Les références aux fonctionnalités Act! se rapportent aux versions Act! Premium et Premium Plus v20.1 et versions supérieures.

1. Définir les données personnelles

Les données personnelles constituent toutes les données qui peuvent être utilisées seules ou combinées avec d'autres données pour identifier une personne. Dans le cadre du RGPD, le terme de « données personnelles » tient compte d'un large éventail d'éléments permettant d'identifier une personne, tels que les noms et numéros d'identification uniques, les adresses IP, les données comportementales en ligne et les données de localisation.

Une grande partie des informations concernant les personnes (par opposition aux informations concernant les entreprises et organisations) que vous enregistrez dans le système CRM sont susceptibles d'être considérées comme des « données personnelles » dans le cadre du RGPD. Il est donc primordial de veiller à ce que la création, le stockage, la gestion et l'utilisation des données soient conformes aux exigences du Règlement. Il est non seulement important de sécuriser les données, mais vous devez également vous assurer qu'elles ne sont conservées que le temps nécessaire.

2. Contrôleurs et processeurs de données

Une organisation qui détermine comment et à quelles fins les données personnelles sont traitées est appelée un « contrôleur ». Un processeur traite des données personnelles pour le compte d'un contrôleur. Le RGPD impose des obligations légales aux contrôleurs. Les processeurs ont quant à eux également des obligations, notamment en ce qui concerne l'archivage des traitements effectués.

3. Champ d'application territorial

Le RGPD s'applique à toutes les organisations établies au sein de l'UE, ainsi qu'aux organisations traitant les données personnelles des citoyens de l'UE, même si l'organisation est en dehors de l'UE.

En enregistrant le pays de résidence d'une personne dans Act!, vous pouvez rapidement identifier les documents entrant dans le cadre du RGPD. Un regroupement de ces fichiers peut également être créé pour une consultation simple et rapide.

Comment créer et gérer les groupes dans Act! : Article 39116

4. Principes de protection des données

Dans le RGPD il existe six principes de protection des données qui régissent la manière dont les données d'une personne peuvent être utilisées. Ces données personnelles doivent être :

- Utilisées équitablement, légalement et de manière transparente.
- Recueillies à des fins précisées, et utilisées d'une manière compatible avec ces objectifs.
- Utilisées d'une manière adéquate, pertinente et limitée à ce qui est nécessaire aux fins spécifiées.

Ces premières exigences sont très étroitement liées. Act! ne peut pas entièrement contrôler ou limiter la façon dont vous utilisez vos données personnelles, mais peut vous aider à :

1 Gardez une trace de la façon dont les utilisateurs créent, modifient et utilisent des informations.

Comment utiliser Liste d'historique dans Act! : Article 39112

2 Limiter l'accès de certains utilisateurs aux données ou à des champs spécifiques en lien avec leur fonction.

Le rôle des sécurités dans Act! : Article 39117

3 Stocker et afficher clairement les préférences des individus stockées dans la base de données sur la façon dont leurs données sont utilisées, afin que les utilisateurs puissent travailler en bonne intelligence avec les données. Les opt-ins ou opt-outs de communications ou d'intérêts spécifiques doivent également être conservés pour que les communications restent pertinentes. Dans l'exemple ci-dessous, les destinataires ont la possibilité de se désinscrire des campagnes e-marketing[1]; vous pouvez consulter une liste des désinscriptions (opt-outs) en suivant les étapes décrites dans l'article ci-dessous :

Comment puis-je créer une recherche de mes rebonds et opt-out Act! emarketing dans Act! version 17.2 et ultérieures : Article 39111

- Conservées seulement aussi longtemps que nécessaire à des fins précises.

Votre entreprise doit déterminer sa propre politique en matière de données obsolètes ou redondantes, et définir les processus permettant d'identifier et de gérer ces données. Act! peut, en pratique, vous aider de plusieurs façons en :

1 Enregistrement automatique de la date de création et la date de la dernière modification de chaque fichier.

2 Création de groupes pour segmenter automatiquement et mettre en valeur les données correspondant à vos critères déterminés.

3 Utilisation de la fonctionnalité de recherche qui permet des recherches complexes en fonction de la date de la dernière modification des différents éléments du fichier client.

4 Définition de paramètres autorisant les utilisateurs à marquer manuellement des données spécifiques pour suppression ou archivage à l'aide d'un champ personnalisé.

L'article suivant vous permet de rechercher des données pour des valeurs de champs spécifiques dans Act! :

Comment faire une recherche dans Act! : Article 39113

Outre la recherche de champs individuels, vous pouvez également créer une recherche à l'aide des fonctions ET/OU :

Comment créer, utiliser et modifier une Requête avancée dans Act! : Article 39118

En plus de rechercher des champs individuels, vous pouvez configurer des groupes. Avec Act!, vous pouvez contrôler quels Contacts sont membres d'un Groupe :

Comment créer et gérer les champs de bases de données dans Act! : Article 39115

• Conservées sous une forme permettant l'identification des personnes concernées, uniquement aussi longtemps que nécessaire.

Créer des dates et éditer les dates des fichiers client peut prouver quand les dernières interactions ont été effectuées. Celles-ci peuvent être utilisées pour générer des rapports ou des recherches qui peuvent ensuite être utilisés pour vérifier s'il est toujours nécessaire de conserver le fichier client. Les utilisateurs peuvent par exemple prendre des décisions en fonction de la date de dernière interaction avec un contact ou de la modification d'un contact.

Vous pouvez suivre les changements de champs en activant le suivi de l'historique pour des champs spécifiques dans votre base de données par le biais de la zone Définir les champs d'Act!, vous permettant d'enregistrer toutes les modifications apportées par n'importe quel utilisateur aux données personnelles :

Comment créer et gérer les champs de bases de données dans Act! : Article 39115

• Traitées de manière à garantir la sécurité des données à caractère personnel, y compris la protection contre les traitements non autorisés et illicites et contre les pertes, destructions ou dommages accidentels. Des mesures techniques et organisationnelles appropriées doivent être mises en œuvre.

Act! offre un large éventail de caractéristiques régissant la sécurité et l'accès aux fichiers. Les fonctionnalités vous permettent de limiter l'accès des utilisateurs aux données en ajustant leur niveau de sécurité ou en appliquant des autorisations spécifiques à un champ. L'accès des utilisateurs peut être limité, ce qui signifie qu'ils n'auront accès qu'aux données les concernant, réduisant le risque de « divulgation ou d'accès non autorisée à des données personnelles ».

Le rôle des sécurités dans Act! : Article 39117

Remarque : Pour déterminer si plusieurs Notes, Historique, Opportunités ou Contacts doivent être Public/Privé, vous avez besoin d'un Client hors-ligne. Vous trouverez plus d'informations sur la création d'un Client hors-ligne dans l'article suivant :

Comment mettre en place mon Client Cloud hors-ligne dans Act! Premium : Article 37973

Act! offre un large éventail de fonctions permettant la gestion des fichiers clients et l'accès aux données :

1 La sécurité au niveau des champs peut être utilisée pour s'assurer que les utilisateurs ne peuvent voir ou modifier que les données du champ en lien avec leur fonction.

Comment gérer les droits d'accès aux champs dans Act! : Article 39114

2 L'accès aux fichiers client peut être stipulé pour les Contacts, Sociétés, Groupes, et Opportunités ; l'ensemble du contenu du fichier client n'étant visible que pour les utilisateurs specifiés ou l'équipe d'utilisateurs configurée.

3 Les données des fichiers client telles que notes, historiques et activités peuvent être définies comme privées, ce qui signifie qu'elles ne sont visibles que par le responsable du fichier client spécifié.

4 Cinq rôles de sécurité utilisateur par défaut offrent une gamme d'autorisations aux fonctions de base de données, allant de la simple navigation à l'administration complète. Ces rôles contrôlent les autorisations telles que l'exportation de données et la création, la suppression ou la modification de fichiers client.

Vous trouverez des informations sur le contrôle de l'accès des utilisateurs sur notre base de connaissances dans les articles suivants :

Comment modifier le statut Public/Privé de Notes, d'Historique ou d'Opportunités multiples : Article 39108

Examinez les rôles des utilisateurs d'Act! et assurez-vous que les rôles de sécurité et l'accès aux fichiers client sont en place pour les utilisateurs en fonction des exigences de leurs rôles individuels :

Comment définir les contrôles d'accès aux contacts pour les utilisateurs dans Act! : Article 39110

La fonction de synchronisation de la base de données, qui permet de créer une base de données distante, peut être basée sur un « ensemble de synchronisation », dans lequel seuls les fichiers de contacts correspondant aux critères spécifiés sont transférés à l'utilisateur distant.

Comment gérer les « ensemble de synchronisation » de base de données distante dans Act! : Article 14072

Afin de modifier un « ensemble de synchronisation » dans une version Cloud d'Act! vous devez soumettre un ticket à notre équipe Cloud, ici.

Un nom d'utilisateur et un mot de passe peuvent être définis pour chaque utilisateur individuel d'Act!. De plus, une politique de mots de passe détaillée peut être configurée dans Act!, afin de déterminer la longueur, la complexité, la fréquence des changements et la réutilisation des mots de passe précédents.

Vous pouvez gérer un utilisateur par le biais de la section Gérer les utilisateurs d'Act! ; vous pouvez également y définir un mot de passe :

Comment créer et gérer des utilisateurs de base de données dans Act! : Article 19474

Comment ajouter ou supprimer des utilisateurs à ma base de données Act! Premium Cloud : Article 37948

Comment gérer les paramètres de complexité de mot de passe : Article 19180

Act! permet la sauvegarde des données pour éviter toute perte, destruction ou dommage accidentel. Cela inclut une fonctionnalité de planification pour automatiser les sauvegardes à une fréquence spécifiée. Ces fonctionnalités doivent être utilisées en conjonction avec une politique de sauvegarde efficace.

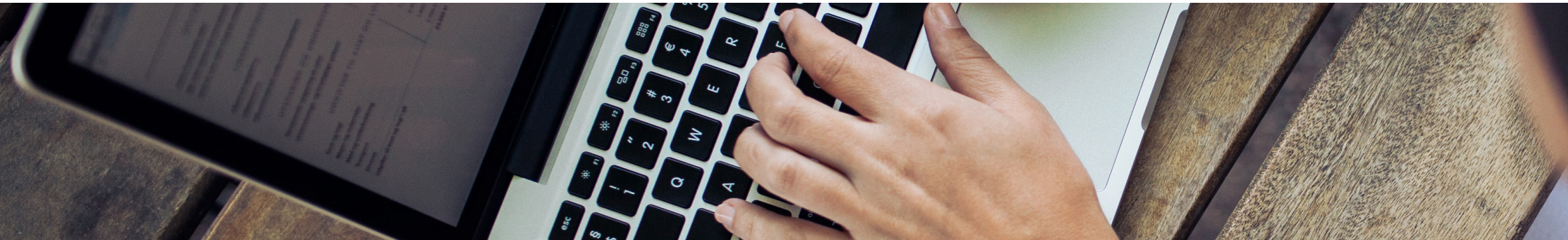
Comment sauvegarder et restaurer une base de données Act! : Article 19211

Comment utiliser le planificateur d'Act! pour sauvegarder automatiquement votre base de données Act! : Article 19218

Si vous utilisez une version Cloud d'Act!, Act! sauvegarde automatiquement les bases de données toutes les 6 heures. Vous trouverez plus d'informations sur les sauvegardes dans les articles ci-dessous :

À quelle fréquence sauvegardez-vous votre base de données Cloud Act! Premium ? : Article 39080

Comment puis-je demander une sauvegarde de ma base de données Cloud Act! Premium ? : Article 39079



5. Base légale du traitement

Les organisations ont besoin d'une base légale pour traiter des données. Il existe six bases légales pour le traitement des données. Dans ce document, nous ne couvrons que la base légale du consentement même si au moins l'une des autres bases est susceptible de constituer une base de traitement aussi pertinente, sinon plus, que le consentement. Voici les bases sur lesquelles une organisation peut s'appuyer :

Le consentement	Les personnes doivent donner ce consentement clairement et en relation avec un processus spécifique.
Le contrat	Le traitement est nécessaire pour un contrat ou pour conclure un contrat.
Les obligations légales	Les individus doivent les accorder spécifiquement, en relation avec un traitement bien précis.
Le intérêts vitaux	Pour sauvegarder la vie d'une personne.
Les tâches publiques	Ceci ne s'applique qu'aux organisations du secteur public.
Les intérêts légitimes	Le traitement est nécessaire pour vos intérêts ou ceux d'autres parties, à moins qu'il n'existe une bonne raison de protéger les données personnelles de l'individu, plus importante que ces intérêts.

Le consentement

Le consentement est souvent utilisé comme base légale pour le traitement à des fins de marketing. Ce doit être une indication libre, spécifique, informée et sans ambiguïté des souhaits de l'individu. Doit être présente une forme d'action affirmative claire ; en d'autres termes, un consentement positif. Ni le silence, ni des cases pré-cochées, ni l'inactivité ne devraient avoir valeur de consentement. Le consentement doit également être distinct des autres modalités et conditions, et vous devez fournir des moyens simples pour que les individus puissent retirent leur consentement. Le consentement doit être vérifiable et vous devez prévoir des méthodes permettant aux personnes d'exercer leurs droits de donner leur consentement.

La section ci-dessous vous aidera à gérer le consentement e-marketing[1] donné par opt-out et opt-in.

---

6. Droits individuels

Le RGPD étend les droits d'un individu sur la façon dont ses données personnelles peuvent être utilisées.

6.1 Le droit d'être tenu informé

Le RGPD oblige les entreprises à informer les individus au moment de la collecte de leurs données. L'étendue des informations que vous fournissez est déterminée par le fait que vous avez obtenu ou non les données personnelles directement auprès des individus. Les informations sur le traitement des données personnelles doivent être :

- Concises, transparentes, intelligibles et facilement accessibles.
- Écrites dans un langage clair et simple, en particulier si ces informations s'adressent à un enfant.
- Gratuites.

Quelles que soient les données que vous recueillez, les individus doivent être tenus à jour. Ils doivent savoir quels renseignements personnels sont conservés et l'utilisation que vous allez en faire. Toute communication avec vos clients à ce sujet doit être simple et gratuite.

Grâce à la personnalisation, un champ peut être créé dans Act! pour enregistrer le fait que les informations appropriées ont été données à la personne dont les coordonnées sont enregistrées dans un fichier de contact. Par exemple, un champ Date ou Oui/Non (case à cocher) peut être créé pour indiquer que l'information appropriée a été donnée et à quel moment.

Une liste déroulante peut préciser la source de la permission accordée (par exemple : appel téléphonique, formulaire de contact Web, etc.)

Comment créer et gérer les champs de bases de données dans Act! : Article 39115

Lorsque vous avez créé un champ, vous recevrez un message vous demandant si vous souhaitez ajouter le champ à votre modèle. Vous trouverez plus d'informations sur la mise en page dans l'article ci-dessous:

Concevoir des mises en page dans Act! : Article 15332

Si vous possédez un site Web, il est alors possible d'ajouter un formulaire Web Act! permettant de fournir un processus de « double consentement » à la personne qui remplit le formulaire avant d'enregistrer le fichier de cette personne en tant que contact dans Act!. Le fait que cette demande ait été soumise par l'individu peut être signalé par le biais d'Act! à des fins de vérification.

Comment utiliser la fonction Formulaires Web dans Act! : Article 37906

Les utilisateurs d'Act! doivent envisager de mettre en œuvre un processus régissant la communication de renseignements aux personnes qui remplissent les formulaires, ainsi que l'enregistrement de la date et de la façon dont ces renseignements ont été fournis.

6.2 Le droit d'accès

Avec le droit d'accès au RGPD, les informations doivent être fournies gratuitement, à moins que la demande ne soit « manifestement infondée ou excessive » et que des frais raisonnables peuvent être facturés. En résumé, les informations doivent être fournies sans délai et dans un délai d'un mois à compter de leur réception. Il existe une obligation de vérifier l'identité de la personne qui fait la demande par le biais de « moyens raisonnables ». Les demandes faites sous forme électronique doivent être présentées dans un format couramment utilisé. Il existe une recommandation sur les meilleures pratiques selon laquelle lorsque cela est possible, les organisations doivent être en mesure de fournir un accès à distance à un système libre-service sécurisé permettant à l'individu d'accéder directement à ses informations. Cela ne conviendra pas à toutes les organisations, mais il existe certains secteurs où ce fonctionnement peut s'avérer efficace.

Act! fournit un rapport de contact détaillé qui peut être comparé à un contact individuel afin de fournir un compte rendu complet des informations stockées le concernant.

Comment exécuter et gérer les rapports dans Act! : Article 14022

Les données contenues dans les champs Contact peuvent également être exportées vers un certain nombre de formats de fichiers (y compris .csv) pour un partage facile avec un client.

Comment exporter vos données de Contact, de Société ou de Groupe à partir d'Act! dans un fichier texte ou un fichier csv : Article 38145

6.3 Le droit à la rectification

Les individus ont le droit de rectifier les données personnelles si elles sont inexactes ou incomplètes. Cela doit être fait dans délai d'un un mois avec la possibilité d'un prolongement de cette période si la demande est complexe. Si aucune mesure n'est prise, une explication devra être fournie au requérant, en mentionnant son droit de porter plainte. Les tiers auxquels des données ont été transmises sont également tenus de rectifier les données.

Act! permet de consigner la demande de rectification, par exemple sous forme d'historique. La date de création de l'historique sera alors enregistrée. Les suivis de demande peuvent être enregistrés en tant qu'historique ou activité supplémentaire pour un utilisateur donné.

Act! peut être utilisé pour consigner le lieu où l'information a été partagée avec un tiers afin de faciliter la prise de contact si cette information doit être effacée.

Un processus doit être mis en place afin d'établir les étapes qu'un employé doit suivre lorsqu'il reçoit une demande de rectification.

6.4 Le droit à l'effacement

Également connu comme le « droit d'être oublié ». Ce droit permet à une personne de demander la suppression de données à caractère personnel lorsqu'il n'existe aucune raison impérieuse de poursuivre le traitement de ces données. Les personnes ont le droit d'avoir leurs données personnelles effacées et d'empêcher leur traitement dans des circonstances spécifiques indiquées dans le RGPD. Les tiers auxquels des données ont été transmises doivent également être informés.

Act! permet la suppression des fichiers de contacts, ce qui à son tour entraînera la suppression de toutes les entrées et données associées au fichier (à moins qu'elles ne soient associées à d'autres contacts subsistants). La suppression est enregistrée dans l'historique de l'utilisateur qui a effectué la suppression, avec indication de la date, de l'heure et du nom du contact.

Act! peut être utilisé pour indiquer où l'information a été partagée avec un tiers afin de faciliter la prise de contact avec ce tiers si ces informations sont effacées. Un processus doit être mis en place concernant toute information transmise à des tiers.

Comment créer manuellement des historiques dans Act! : Article 38835

6.5 Le droit de restreindre le traitement

Les personnes physiques ont le droit de bloquer le traitement des données personnelles. Lorsque le traitement est restreint, vous êtes autorisé à stocker les données personnelles, mais non à les traiter ultérieurement. Vous pouvez conserver la quantité minimale suffisante d'informations sur la personne pour vous assurer que la restriction sera respectée à l'avenir.

Un champ personnalisé peut être utilisé pour suivre les préférences du client en matière de non-traitement. Les utilisateurs d'Act! doivent s'y conformer manuellement.

Comment créer et gérer les champs de bases de données dans Act! : Article 39115

Par mesure de précaution supplémentaire, les coordonnées telles que les numéros de téléphone et les adresses e-mail peuvent être déplacées hors des champs par défaut pour éviter par exemple tout contact accidentel ou inclusion dans une campagne e-mail. Vous pouvez déplacer les données vers d'autres champs personnalisés qui ne seront pas lus par Act! afin d'éviter toute inclusion accidentelle.

Comment puis-je utiliser les options Remplacer, Echanger et Copier dans Act! : Article 38137

6.6 Le droit à la transférabilité des données

Les individus peuvent obtenir et réutiliser leurs données personnelles à leurs propres fins dans différents services. Le processeur a un délai d'un mois pour répondre à la requête. Les individus doivent pouvoir transférer ou copier des données d'un service informatique vers un autre, de manière sécurisée et sans entrave. Les données personnelles doivent être fournies dans un format ouvert et structuré, couramment utilisé et lisible par machine. Si cela est techniquement possible, il se peut que vous deviez transmettre les données à une autre organisation. Vous ne devez pas porter atteinte aux droits d'autrui, par exemple en divulguant des données de tiers.

6.7 Droit d'opposition

Du point de vue de l'utilisation d'Act!, les droits pertinents auxquels les individus peuvent s'opposer sont :

- Le traitement fondé sur des intérêts légitimes (y compris le profilage)
- Le marketing direct (y compris le profilage).

Si un processeur traite des données à caractère personnel pour l'exécution d'une tâche légale ou dans l'intérêt personnel de l'organisation, une personne peut s'y opposer pour « motifs liés à sa situation particulière ». L'organisation doit alors mettre fin au traitement, à moins qu'il n'existe des raisons impérieuses et légitimes pour le traitement qui l'emportent sur les droits de l'individu, ou que le traitement ne soit destiné à l'exercice de droits légaux.

Les personnes doivent être informées de leur droit de s'opposer au moment de la première communication et dans l'avis de confidentialité. Cette communication doit être portée explicitement à l'attention de la personne concernée et être présentée clairement et indépendamment de toute autre communication.

Si les activités de traitement sont exécutées en ligne, il doit exister une possibilité pour les individus de s'opposer en ligne.

Avec Act! emarketing et Act! emarketing[1], les destinataires ont la possibilité de se désinscrire dans le bas de page de l'e-mail reçu dans le cadre de votre campagne. L'impact de cette situation est expliqué dans cet article.

Si un client se retire de mes campagnes d'e-marketing, est-ce que le système m'empêche de lui envoyer mes campagnes ou dois-je supprimer l'e-mail du contact de ma base de données ? : Article 38681

Si vous utilisez Act! emarketing[1], vous pouvez suivre les destinataires qui ont choisi de se désinscrire de vos campagnes en suivant les étapes de l'article ci-dessous :

Comment puis-je créer une recherche de mes rebonds et opt-out Act! emarketing dans Act! version 17.2 et ultérieures : Article 39111

Si vous utilisez Act! emarketing[1], vous pouvez consulter vos désinscriptions en suivant les étapes de l'article ci-dessous :

Comment accéder à votre liste d'opt-outs Act! emarketing : Article 28591

Les destinataires peuvent-ils s'inscrire à nouveau à mes campagnes ?

Si votre destinataire se désinscrit par erreur ou s'il souhaite recevoir à nouveau vos e-mails, il peut choisir de s'engager à nouveau dans vos campagnes. Vous devez suivre le processus détaillé dans l'article ci-dessous pour supprimer la désinscription :

Comment puis-je supprimer les e-mails rebonds/opt-outs de ma base de données Act! : Article 37150

Comment importer une liste existante de désinscrits dans Act! ?

Si vous avez déjà utilisé un autre service e-marketing[1] ou si vous avez conservé une liste manuelle de vos désinscriptions, vous pouvez nous les fournir en format CSV en contactant le support technique et nous ajouterons cette liste à votre compte. Nous vous confirmerons que la liste de vos opt-outs a bien été ajoutée à votre compte.

Nous contacter : https://www.act.com/fr-fr/contact

Bien que ce qui précède vous aidera à gérer les opt-outs de vos campagnes, Act! peut également être utilisé pour vous permettre de suivre les désinscriptions d'autres méthodes de contact telles que les SMS ou le courrier postal. Des champs personnalisés dans Act! sont disponibles à ces fins. Vous trouverez des informations sur la création de rubriques personnalisées et leur ajout à votre mise en page dans les deux articles ci-dessous.

Comment créer et gérer les champs de bases de données dans Act! : Article 39115

Concevoir des mises en page dans Act! : Article 15332

6.8 Gestion des opt-outs et des opt-ins

Bien que les destinataires des campagnes d'e-marketing[1] puissent se désabonner et être exclus de vos futures campagnes, il se peut que vous deviez adapter votre base de données pour éviter une inclusion accidentelle dans une fusion de courrier. Pour contourner cela, il suffit de créer un champ e-mail supplémentaire, lors de l'envoi d'un publipostage ou d'une campagne emarketing[1], Act! vérifiera le champ e-mail par défaut. Par exemple, si un client se retire de votre communication marketing, vous devrez peut-être conserver l'adresse électronique du client pour lui envoyer des factures. Le champ personnalisé peut être utilisé pour stocker l'adresse e-mail du client en utilisant la fonctionnalité dans Act! comme expliqué dans l'article suivant :

Comment utiliser les options Remplacer, Échanger et Copier dans Act! : Article 38137

Si vous utilisez la méthode ci-dessus, vous pouvez démarrer ce processus en accédant à votre liste de désinscriptions. Vous pouvez y accéder en utilisant l'une des deux méthodes de l'article ci-dessous, pour Act! emarketing[1] ou Act! emarketing :

Comment puis-je créer une recherche dans mes désinscriptions e-marketing[1] dans Act! v17.2 et versions ultérieures ?

Comment accéder à votre liste d'opt-outs dans Act! emarketing : Article 28591

6.9 Droits relatifs à la prise de décision et au profilage automatisés

Le RGPD donne des droits aux individus lorsqu'ils font l'objet d'une prise de décision automatisée et d'un profilage automatisé. Ces droits sont plus forts lorsque la prise de décision et le profilage automatisés ont un effet légal ou sont d'une importance similaire pour l'individu.

Les administrateurs d'Act! doivent s'assurer que leurs conseillers commerciaux et juridiques comprennent qu'il est possible d'automatiser la prise de décision et le profilage grâce à Act!. Des avis appropriés doivent être inclus dans les avis de confidentialité. Les processus pertinents doivent être pris en compte, par exemple pour arrêter de prendre des décisions automatisées et de profiler une personne dans les circonstances requises, pour permettre aux utilisateurs d'Act! de fournir aux clients leurs données utilisées pour la prise de décision et le profilage automatisés et, enfin, pour signaler les contacts appartenant à la catégorie « groupe vulnérable », telle que définie dans le cadre du RGPD.

Le domaine d'Act! ayant trait à la prise de décision automatisée est celui des tâches AutomAct!. Il est de votre responsabilité de vous assurer que les étapes des AutomAct! soient mises à jour régulièrement afin d'éviter une violation potentielle du RGPD. Par exemple un client ayant choisi de ne plus recevoir vos e-mails pourrait recevoir un e-mail automatisé dans le cadre des étapes de votre tâches AutomAct! si les renseignements contenus dans son fichier client ne sont pas à jour.

Plusieurs exemples de tâches AutomAct! sont disponibles dans Act!. Vous trouverez plus d'informations à ce sujet dans les articles ci-dessous :

Qu'est-ce que les tâches AutomAct! dans Act! : Article 37910
Comment créer et gérer des tâches AutomAct! dans Act! : Article 26944

7. Responsabilité et gouvernance

Le RGPD exige que les organisations mettent en place des mesures de gouvernance globales mais proportionnées. Pour démontrer la conformité, une organisation doit mettre en œuvre des mesures techniques et organisationnelles appropriées (voir ci-dessous) qui garantissent et démontrent que vous êtes conforme. Cela peut inclure des politiques internes de protection des données telles que la formation du personnel, des audits internes des activités de traitement et l'examen des politiques internes en matière de ressources humaines.

- Tenir à jour la documentation pertinente sur les activités de traitement ;
- le cas échéant, désigner un délégué à la protection des données
- utiliser, le cas échéant, des évaluations d'impact sur la protection des données ;
- mettre en œuvre des mesures qui respectent les principes de la protection des données dès la conception et de la protection des données par défaut. Ces mesures pourraient inclure :
    - la minimisation des données ;
    - la « pseudonymisation » ;
    - la transparence ;
    - permettre aux individus de surveiller le traitement ; et
    - la création et l'amélioration constante des fonctions de sécurité.

Les organisations peuvent également adhérer à des codes de conduite et/ou des systèmes de certification approuvés.

Documentation

Dans le cadre du RGPD, vous pouvez être tenu de produire des preuves de conformité. Vous pouvez y contribuer en documentant les décisions que vous avez prises au sujet de l'utilisation des données personnelles.

Act! comporte un certain nombre de caractéristiques qui peuvent vous aider à consigner les décisions prises concernant l'utilisation des données personnelles :

- Établissement de la source d'un fichier client via un champ spécifiquement dédié à cet effet.
- Joindre des pièces justificatives à un document, comme la correspondance par e-mail, les documents numérisés et les enregistrements des appels.

Comment joindre un document à un Contact, Groupe, Société, ou Opportunité dans Act! : Article 39109

- La note horodatée et les données historiques peuvent être enregistrées par individu, en enregistrant une interaction avec elle ou en marquant un processus interne qui a été suivi.

Comment utiliser Liste d'historique dans Act! : Article 39112

- Configurer les champs pour enregistrer automatiquement une entrée d'historique lorsque leur contenu est modifié, permettant ainsi la traçabilité des modifications.

Comment créer et gérer les champs de bases de données dans Act! : Article 39115

Act! peut vous aider à documenter la conformité en fournissant la capacité de stocker des preuves d'activités de traitement conformes. Par exemple, une entrée dans l'historique peut être faite par l'utilisateur, ou un fichier peut être stocké dans l'onglet Documents (par exemple une page d'archive html du formulaire de collecte de données approprié). Cela nécessitera une formation des utilisateurs sur les exigences de conformité et la façon dont ces exigences influent sur l'utilisation d'Act!.

En outre, un utilisateur pourrait stocker de la documentation interne, par exemple des procédures d'exploitation standard dans Act! soit sous forme de pièces jointes dans des fichiers client, soit sous forme de nouveaux menu contextuels – vers, par exemple, des documents individuels stockés à l'extérieur d'Act!.

L'article suivant explique comment créer un historique et joindre un document/fichier pertinent :

Comment créer manuellement des historiques dans Act! : Article 38835

Les organisations comptant moins de 250 employés doivent conserver des dossiers sur les activités de traitement à haut risque telles que le traitement de données qui peuvent entraîner un risque pour les droits et libertés des personnes, ou des catégories spéciales de données, voire des données relatives à des infractions pénales. Comme mentionné ci-dessus en ce qui concerne la conformité, Act! peut être utilisé afin de stocker des documents dans des circonstances appropriées.

Protection des données dès la conception et par défaut

Les processeurs ont l'obligation générale de mettre en œuvre des mesures techniques et organisationnelles pour montrer qu'ils ont pris en compte et intégré la protection des données dans leurs activités et dans le processus de traitement des données.

Le respect de la vie privée dès la conception est une approche des projets qui met en avant dès le départ le respect de la vie privée et la conformité à la protection des données... Les organisations doivent veiller à ce que le respect de la vie privée et des données soit une considération essentielle dès les premiers stades de tout projet, puis tout au long de son cycle de vie. Par exemple, lors de :

- La mise en place de nouveaux systèmes informatiques pour le stockage ou l'accès aux données personnelles ;
- L'élaboration de lois, de politiques ou de stratégies ayant des répercussions sur le respect de la vie privée ;
- Le lancement d'une initiative de partage de données ; ou
- L'utilisation des données à de nouvelles fins.

Une évaluation de l'impact sur la protection des données doit être effectuée lorsque l'utilisation de nouvelles technologies est envisagée. Le Commissaire à l'information britannique possède un code de pratique expliquant la mise en œuvre des évaluations d'impact. L'exécution d'un tel programme doit viser à réduire les risques de préjudice pour les personnes en raison de l'utilisation abusive de leurs données personnelles. Un tel programme peut également vous aider à concevoir des processus plus efficaces et plus rapides pour le traitement des données personnelles.

Dans ce scénario, Act! est plus susceptible d'être utile comme archive de documents. Par exemple, si des « Projets » ont été créés en tant qu'entité en utilisant le Gestionnaire de Tables Personnalisées dans Act! Premium Plus, l'analyse d'impact écrite pour chaque projet peut être stockée avec d'autres documents, comme une analyse de rentabilisation pertinente ou un document de lancement de projet.

Qu'est-ce que les tables personnalisées dans Act! Premium Plus ? : Article 38976

Chaque organisation doit mettre en œuvre des processus de conformité, en documentant par exemple la conformité et en réalisant des évaluations d'impact. Elles doivent également adopter des procédures pertinentes pour mettre en place les mesures, afin de respecter les principes de protection des données dès la conception et par défaut. Les organisations doivent, le cas échéant, travailler avec des consultants pour s'assurer qu'elles mettent en place et maintiennent les mesures de gouvernance appropriées.

8. Désignation d'un délégué à la protection des données

Cette nomination est requise dans certaines circonstances. Qu'une organisation soit obligée ou non de nommer un délégué à la protection des données (DPD), elle doit disposer de compétences et de ressources suffisantes pour se conformer au RGPD et aux autres obligations pertinentes en matière de protection de la vie privée. Les tâches minimales requises du DPD doivent être définies.

9. Sécurité des données personnelles

Les données à caractère personnel doivent être traitées en toute sécurité en prenant les mesures techniques et organisationnelles appropriées. Vous devez procéder à une analyse des risques proportionnée et mettre en place des politiques organisationnelles pertinentes et prendre les mesures techniques et physiques appropriées. L'anonymisation et le cryptage doivent être envisagés. Les systèmes et les services doivent assurer la confidentialité et la sécurité des données personnelles et maintenir leur intégrité. Des sauvegardes doivent être effectuées pour permettre la restauration des données perdues. Quelles que soient les mesures mises en place, elles doivent être testées et toutes les améliorations nécessaires doivent être apportées.

Transfert de données en dehors de l'UE

Les données personnelles ne peuvent être transférées que lorsque les conditions spécifiées sont remplies.

Un certain nombre de régimes ont été mis en place par des organismes de réglementation, à la suite de décisions de la Commission européenne.

Des exceptions à l'interdiction générale existent dans certaines circonstances bien précises - lorsque le transfert est :

- effectué avec le consentement éclairé de l'individu ;
- nécessaire à l'exécution d'un contrat entre l'individu et l'organisation ou de mesures précontractuelles prises à la demande de l'individu ;
- nécessaire à l'exécution d'un contrat conclu dans l'intérêt de la personne, entre le responsable du traitement et une autre personne ;
- nécessaire pour des raisons importantes d'intérêt public ;
- nécessaire à l'établissement, à l'exercice ou à la défense de revendications légales ;
- nécessaire à la protection des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée est physiquement ou juridiquement incapable de donner son consentement ; ou
- effectué à partir d'un registre qui, en vertu de la législation britannique ou européenne, est destiné à fournir des informations au public (et qui peut être consulté soit par le public en général, soit par ceux qui sont en mesure de démontrer un intérêt légitime à consulter le registre).

Avis d'atteinte à la vie privée

Les organismes de traitement des données ont l'obligation de notifier les atteintes à l'organisme de contrôle concerné si ces dernières sont susceptibles d'entraîner un risque pour les droits et libertés des personnes - une atteinte qui, si rien n'est fait, aura un impact préjudiciable significatif sur les individus : sous la forme par exemple d'une discrimination, d'une atteinte à la réputation, d'une perte financière, d'une perte de confidentialité ou tout autres désavantages économiques ou sociaux importants. Les personnes concernées doivent également être avisées en cas de risque élevé.

La notification doit être faite aux autorités de surveillance dans les 72 heures et, si nécessaire, aux personnes sans retard injustifié. Ne pas le faire peut entraîner une amende conséquente, allant jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires mondial.

Vous devez prendre des mesures pour former le personnel sur les exigences de notification et mettre en place des mesures pertinentes pour identifier les violations internes, mener des enquêter à leur sujet et en rendre compte.

Application du RGPD aux mineurs

Si votre entreprise propose ses produits ou services aux mineurs, vous devez sans doute obtenir le consentement de leurs parents ou de leurs tuteurs avant de recueillir ou de traiter leurs données. Dans le cadre du RGPD, seule une personne âgée de 13 ans ou plus peut donner son propre consentement.

Act! CRM vous permet d'enregistrer l'âge de chaque nouveau contact, et d'effectuer une recherche pour identifier les mineurs pour lesquels vous avez un fichier client. Vous pouvez ensuite prendre les mesures appropriées pour traiter les informations relatives à ces mineurs conformément aux exigences du RGPD.

A propos d'Act!

Act! facilite la gestion des relations clients sur le long terme avec un accès rapide et organisé à toutes vos données client. Parce que chaque entreprise fonctionne différemment, Act! est spécialement conçu pour vous donner une grande liberté de personnalisation et vous offre ainsi un espace de travail flexible, accessible, et connecté.

Act!, une solution CRM qui vous ressemble.

Pour en savoir plus sur Act!, rendez-vous sur
www.act.com/fr

Ou contactez-nous au
09 75 18 23 09 (France)
078 483 840 (Belgique)

Suivez-nous sur

1 Les serveurs Act! emarketing sont situés aux États-Unis. Le transfert de données vers ces servers est conforme au RGPD. Si vous utilisez Act! emarketing, veuillez vous assurer de vous conformer au RGPD en notifiant vos destinataires que leurs données seront transférées aux États-Unis.

Act! International Limited | Ground Floor, Q15 Quorum Business Park | Benton Lane, Newcastle upon Tyne | NE12 8BU | act.com/fr