

Annexe 1 : Conformité au Règlement Général sur la Protection des Données (RGPD)

1.1 Assurer la protection des données privées – Conformité RGPD

Le Règlement Général sur la Protection des Données (RGPD) est applicable depuis le 25 mai 2018. Il ajoute de nouvelles obligations pour l'entreprise et introduit de nouveaux concepts : principe de transparence, information des consommateurs, « privacy by design », rôle de « Data Protection Officer », mesures techniques et organisationnelles et... sanctions !



Cette nouvelle réglementation européenne impacte les responsabilités de chacun, l'organisation, l'ensemble des prestataires et bien entendu les outils informatiques. Nous travaillons régulièrement aux mises à jour réglementaires de la solution CRM afin, non seulement de la rendre conforme aux exigences européennes, mais aussi, de mettre à votre disposition les outils d'assurance et de prévention nécessaires.

1.1.1 ETRE EN CONFORMITE AVEC E-DEAL CRM BY EFFICY

E-DEAL CRM BY EFFICY offre de nombreuses possibilités pour respecter le droit européen et protéger ses données privées.

Sécurité

- Une solution SaaS hébergée à 100% dans l'Union Européenne
- Des datacenters certifiées ISO 27001 et des sites audités en permanence
- Une sécurisation des flux : protocoles HTTPS, SFTP, FTPS, IMAPS, POPS
- La mise en place de VPN ou de liens directs type MPLS avec le SI

Solutions

- Une gestion du consentement : abonnements/désabonnements, extraction de données, effacement ou randomisation des données, opposition au profilage, portabilité
- La possibilité de définir des tâches automatiques de conservation des données
- Des services intégrés avec des solutions partenaires dans l'UE

Accès

- Une définition des droits utilisateur par profils et propriété de la donnée métier
- Une sécurisation de l'authentification et une politique de mot de passe
- L'identification de comptes utilisateurs inactifs, la désactivation de comptes

Approche

- Une solution conçue dans un contexte juridique encadrant la protection des données
- Une approche « privacy-by-design » assurant maîtrise des processus et collecte active des données
- DPO E-DEAL : application du règlement, documentation, conseil, formations, etc.
- Un service juridique en France et un partenaire spécialisé FGConseil.fr



1.1.2 DISPOSITIF ORGANISATIONNEL

En tant que fournisseur, E-DEAL CRM BY EFFICY est responsable de la protection des données au même titre que chacun de ses clients. Pour cela, les dispositions suivantes sont mises en place :

- Définition des rôles et des périmètres d'intervention de chacun
- Mise en place de compte utilisateurs à tous les niveaux : logiciel, système, outils (pas de compte root typiquement)
- Gestion des arrivées et départs des intervenants du projet
- Documentation et partage de connaissance à l'ensemble des intervenants
- Sensibilisations régulières aux bonnes pratiques de sécurité

Efficacy accompagne votre DPO dans la documentation du traitement des données personnelles : identification des données, définition des traitements et cartographie des flux. Efficacy est un organisme de formation agréé et dispense des formations sur les modules standards de sa solution mais également sur les paramétrages locaux réalisés pour les besoins de nos clients.

1.1.3 HEBERGEMENT DES DONNEES

La solution E-DEAL CRM BY EFFICY en mode SaaS est entièrement hébergée dans **l'Union Européenne**. Il n'existe pas de flux de données transféré dans un pays hors UE. Le logiciel E-DEAL CRM BY EFFICY intègre toutefois des connecteurs avec des solutions tiers pouvant être hébergées hors de l'union européenne (Amérique du Nord : Google Maps, Hootsuite par exemple). Pour autant, les données privées ne sont pas échangées avec ces systèmes.

Les plates-formes SaaS sont certifiées ISO 27001 et situées dans 2 Datacenter professionnels classés Tiers 3+. Les données sont sauvegardées en permanence, conservées et cryptées sur des baies NAS indépendantes de la production. Les accès physiques aux datacenters respectent toutes les normes de sécurité en vigueur pour assurer la protection du service : salles privatives et distantes, habilitations, badges et points de contrôles, video-surveillance, et gardiennage.

1.1.4 PRIVACY BY DESIGN

La réglementation européenne (RGPD) impose une conception de la protection des données dès la conception afin de minimiser le périmètre des données.

La collecte **active** des données personnelles est entièrement paramétrable et réduite à son strict minimum en standard. L'administrateur peut à tout moment altérer les formulaires de saisies des données personnelles afin de ne collecter que les informations nécessaires au traitement.

Concrètement si l'on a besoin de connaître l'âge de la personne, il est possible de paramétrer un champ « Année de naissance » qui sera suffisant pour connaître / estimer l'âge plutôt que de collecter le jour et le mois de naissance. Lors de la conception de la solution, l'étape de recueil du dictionnaire de données intègre l'étude d'impact du recueil



des données personnelles : motif de collecte, traitement associé, étude d'impact, piste de minimisation.

Certaines fonctions du logiciel entraînent une collecte **passive** des données, c'est-à-dire sans action implicite demandant la collecte de la part de l'acteur du traitement : géolocalisation, RNVP, tracking web, réseaux sociaux ou calcul de meta-données. Toutes ces fonctions sont désactivées par défaut et peuvent être activées par un administrateur lorsqu'un traitement le nécessite.

1.1.5 SECURISATION DES DONNEES

Architecture

Le chapitre « Sécurité et confidentialité » de notre proposition présente les mesures de sécurisation de la solution. Parmi celles-ci, nous pouvons citer :

- Sécurisation de l'identification de l'utilisateur : protection par login / mot de passe, cryptage du mot de passe, possibilité d'utiliser une authentification déléguée à l'annuaire ou un système de Single-Sign-On.
- Politique de mot de passe : vérification des caractères, changement de mot de passe régulier
- Sécurisation des flux : utilisation des protocoles HTTPs, SFTP, mise en place de VPN
- Sécurisation des accès : définition de profil utilisateur, identification des comptes inactifs, gestion de droits détaillée par profil et par traitement.
- Sécurisation de l'infrastructure : sécurité des systèmes, sécurité physique (cf. Chapitre hébergement)

Cas des réseaux sociaux et du medias web

E-DEAL CRM BY EFFICY intègre des fonctions liées aux réseaux sociaux grands publics tels que LinkedIn, Facebook ou Twitter. Ces fonctions peuvent être activées par l'administrateur ou l'utilisateur et ne stockent pas directement les informations issues des réseaux sociaux : c'est la session de l'utilisateur ou de la société sur le réseau social en question qui accède à la donnée en lecture via les API proposés par les réseaux sociaux.

Plusieurs fonctions du logiciel sont liées au media web. Certaines font appel à un service de Hub multi-tenant en ligne (tracking, short URL service, enquêtes en ligne, bibliothèque d'images) : ce service multi-tenant a été conçu dès le début de manière sécurisée : aucune donnée personnelle n'est stockée dans le Hub E-DEAL, des tokens techniques sont utilisés afin de récupérer les données.

1.1.6 DROIT DES PERSONNES

La réglementation européenne a étendu les droits des personnes vis-à-vis du stockage et du traitement des données personnelles.

- Consentement : la solution intègre la fonction d'opt-in / opt-out sur tous les canaux marketing



- Portabilité des données : il est possible à tout moment d'extraire un « dossier client » dans un format bureautique
- Durée de conservation des données à caractère personnel : il est possible de customiser des règles de conservation très précises et en lien avec le métier (date de dernière contact, date de mouvement des données, délais, etc.)
- Effacement et Droit à l'oubli : la solution permet de customiser des règles d'anonymisation des données afin d'assurer l'effacement des données personnelles tout en conservant l'historique de l'activité pour le reporting (nombre de contacts, nombre de dossiers, délais de traitement, etc.)
- Opposition (prospection, profilage) : l'outil permet de définir des filtres de ciblage et de reporting afin de ne pas prendre en compte les personnes s'opposant à ce type de traitement.

Notez également qu'E-DEAL CRM BY EFFICY peut tout à fait être « sourcé » par une solution de référentiel de pilotage dans une logique de projet de gouvernance des données (<http://www.meta-analysis.fr> par exemple).

1.1.7 PILOTER LES REGLES DE PROTECTION DES DONNEES

E-Deal CRM by Efficacy a conçu le Data Privacy Center à cet effet afin de maîtriser toutes les règles appliquées à la protection des données personnelles et de les gérer en un point central du module administrateur.

De nombreuses aides et facilitateurs font ainsi leur apparition :

- Archivage des contacts

La notion d'archivage des personnes et silhouettes a été revue : une personne archivée ne remonte plus dans les résultats de recherche des fiches Personne et il n'est pas possible d'enrichir une fiche déjà archivée.

Mme Floriane AUGUSTIN		[Archivée le 04/06/2019]			
Assistant de direction chez Canadian Travelers depuis le 18/02/2019					
Service	Direction	?	Adresse pro.	25 Isabella St.	
Fonction	Assistant de direction	?		M4Y 1M7 TORONTO	
				Canada	

Exemple de fiche archivée

- Anonymisation des contacts

Une personne anonymisée est archivée et les données personnelles sont floutées ou vidées (selon le type de données) afin que l'identité de la personne ne soit plus reconnaissable. Le processus d'anonymisation traite également l'historique de relation



client afin d'anonymiser les champs pouvant contenir des informations personnelles (e-mail, pièces jointe, commentaires, meta-données, etc.)

- Demande d'anonymisation

La fonction d'anonymisation est manuelle mais peut aussi être automatisée en fonction d'un calcul de « date de dernier mouvement ». Dans tous les cas, un petit workflow manuel peut être activé pour valider les fiches anonymisés, autrement l'anonymisation est faite automatiquement en fonction d'une durée d'inactivité paramétrable (2 ans par défaut).

Mme MO6aV5 Lt8kmDly [Archivée le 29/01/2019] [Anonymisée le 29/01/2019]

Exemple de fiche anonymisée

- Date de dernier mouvement

Une date de dernier mouvement est calculée par batch toutes les nuits afin de calculer le dernier contact significatif de chaque personne. En fonction de cette date, l'anonymisation peut être lancée automatiquement (Ex : 3 ans sans contact). Ce calcul prend en compte les dernières interactions, les demandes, les réactions aux e-mailing et peut être adapté au cas par cas si nécessaire.

- Données personnelles

Les champs représentant des données personnelles (e-mail, carte d'identité, date de naissance, etc.) peuvent être tagués. Une règle d'anonymisation peut être associée à chaque donnée personnelle éte en fonction du type de champ : flouter ou vider l'information.

Par exemple, il sera probablement nécessaire de flouter des champs « obligatoires » (nom, prénom ou tout autre en fonction des règles métier) et vider des champs « optionnels » (numéro de portable)

- Tentatives de connexions

Il est désormais possible de bloquer temporairement ou définitivement un compte utilisateur au bout d'un certain nombre d'échecs d'authentification. Un compte bloqué peut être réactivé par un administrateur.

- Journal d'événements

Reposant sur le moteur de règle, le journal d'événement permet de tracer les actions sensibles en lien avec la sécurité des données : Exports de données personnelles (population, export excel, reporting excel, requester), modification/suppression des comptes utilisateurs, authentification.

- Data Privacy Center

Tous ces paramétrages et configurations en lien avec la protection des données personnelles sont regroupés au sein d'une fonction dédiée dans le module administrateur.



CENTRE DE DONNÉES PRIVÉES

Le centre de protection des données vous permet de visualiser et modifier, dans un endroit centralisé, les paramètres et fonctions de gestion et de suivi des données privées dans votre application.

Vous trouverez quatre rubriques :

- Date de dernier contact
- Archivage
- Anonymisation
- Journal d'événements

DATE DE DERNIER CONTACT

ARCHIVAGE

ANONYMISATION

JOURNAL D'ÉVÉNEMENTS

?

La fonction d'archivage peut être globalement activée ou désactivée. Et il y a une tâche planifiée qui peut archiver automatiquement les personnes, en fonction de leur "fraicheur", vous pouvez en choisir les paramètres.

L'anonymisation étant destructrice de données, vous avez un contrôle poussé dessus. Les utilisateurs ne peuvent pas anonymiser directement les fiches personnes. Ils peuvent faire des demandes d'anonymisation. Une tâche planifiée va ensuite traiter les demandes, et anonymiser effectivement les fiches Personne. Il y a aussi une autre tâche planifiée qui peut générer automatiquement des demandes d'anonymisation des personnes, en fonction de leur "fraicheur".

Vous pouvez choisir les champs de Personne, Interaction, Opportunité et Demande qui doivent être modifiés/vidés lors de l'anonymisation.

Vous pouvez calibrer, dans le détail, le processus d'anonymisation. Et vous pouvez choisir les paramètres deux tâches planifiées : celle qui génère automatiquement des demandes d'anonymisation, et celle qui traite les demandes en anonymisant effectivement les fiches Personne.

Champs concernés par
l'anonymisation

Demande : 9 Champs
LoyaltyLog : 1 Champs
Interaction : 14 Champs

Demandes
d'anonymisation

0 demandes non traitées

Paramétrage des règles d'anonymisation

1.1.8 ACCOMPAGNEMENT ET VEILLE JURIDIQUE

Efficy peut intervenir une journée par an à compter de la date de mise en production pour aider vos équipes à suivre les évolutions de la réglementation applicable et pour sensibiliser les acteurs clés dont le DPO (10 personnes maximum). E-DEAL CRM BY EFFICY s'engage à informer durant toute la durée du marché en cas de changement de la réglementation.

