Le RGPD, un véritable soulagement pour Dial Once

Dès fin 2015, lors du lancement de notre activité on a fait de la sécurité et de la confidentialité des données notre fer de lance. [...] Il était essentiel pour nous de bien faire voir à nos clients Entreprise que c'est un sujet critique pour Dial Once.

— Charles Dunston, CEO, Dial Once

Le mariage du Numérique et de la Relation Client

Charles Dunston est un Serial entrepreneur, 22 ans après sa première startup en 1996 et à son quatrième essai, il garde un point commun à toutes ses expériences : le digital et la relation client.

Homme aux compétences multiples, à la fois ingénieur en informatique et homme d'affaires avec un cursus HEC, il a toujours su surfer sur la vague au bon moment. Il se lance à l'aube des années 2000 dans l'aventure de la Web Agency avec une base de données au coeur de son offre, puis vient le lancement du 118 000, une aventure avec également une forte dimension technique suivie en 2008 par Chronoresto, une société de livraison de repas à domicile revendue en 2013 aux Pages Jaunes. Sur les deux dernières expériences, la gestion client au travers de call centers est un élément non négligeable, une fonction d'ailleurs rapidement maîtrisée en interne.

Magie du Numérique : Start-up avec Business Modèle découplé

Puis l'aventure Dial Once débute dès 2014 avec comme objectif échapper à l'éternel serveur vocal interactif sur lequel on tombe dès que l'on appelle une entreprise ou une administration. Eviter donc une expérience encore trop souvent frustrante grâce à une interface visuelle plus agréable et plus facile pour faire aboutir sa requête. Second effet de Dial Once, une économie substantielle côté entreprise car la nouvelle autonomie de l'appelant permet de la soulager d'un support téléphonique souvent onéreux.

A un flux de personnes appelant, un contenu digital est donc proposé sous la forme de FAQ, Chatbot ... puis si besoin est, une mise en relation avec un opérateur est réalisée avec la conservation du contexte de navigation de l'appelant afin qu'il ne soit pas obligé de repartir à zéro dès qu'il est en ligne. Une offre qui s'étend aujourd'hui à d'autres points de contact, sites ou autres, via une rubrique du type « Contactez-nous ». Que vous appeliez d'un smartphone équipé de la technologie Dial Once ou non, vous êtes directement redirigé vers une interface visuelle ou vous recevez un sms afin que vous puissiez l'activer, ou encore si vous cliquez sur un numéro de téléphone sur un site, elle sera activée à ce moment-là. Dial Once est en quelques sortes un Hub universel via une interface visuelle.

Sans Sécurité, pas de Business

L'utilisateur reste anonyme car n'est conservé qu'un GUID et la seule donnée qui pourrait être personnelle dans un tel contexte de surf reste le numéro IP. Cependant pour améliorer sa prise en main, l'utilisateur pourrait désirer saisir certaines informations pour profiter d'une approche plus personnalisée et alors là de nombreuses informations personnelles seraient à prendre en compte. Alors que la clientèle de Dial Once est essentiellement Grand Compte dans des domaines tels que la finance, les assurances ou en-

core l'administration publique, l'aspect sur la sécurité et la confidentialité des données est au coeur de l'activité de la société. Sans une confiance absolue des clients, il n'y a pas de business possible pour Dial Once : « *Dès fin 2015, lors du lancement de notre activité on a fait de la sécurité et de la confidentialité des données notre fer de lance. On s'est rapproché de la CNIL dès le démarrage. Il était essentiel pour nous de bien faire voir à nos clients Entreprise que c'est un sujet critique pour Dial Once.* » affirme Charles Dunston.

RGPD : Conformité et Valeur Ajoutée

Aujourd'hui le CEO et fondateur de la société est un homme heureux car le RGPD est une véritable aubaine pour une société telle que la sienne : « *C'est une véritable valeur ajoutée. Les données privées sont critiques pour tous nos clients mais selon leur secteur d'activité, nos contrats varient en même temps que les niveaux d'exigence. Avec la conformité au RGPD, nous prouvons non seulement que la sécurité et la confidentialité des données privées sont respectées mais cela nous permet également d'apposer une norme aux différents niveaux d'exigence.* »

Il y a 18 mois, Dial Once a pris les devants et nomme un DPO pour être fin prêt dès le 25 mai 2018. Un DPO déclaré à la CNIL qui en fait son référent. Et pourtant, en tant que sous-traitant, elle n'était pas obligée de se conformer à cette exigence mais le CEO a estimé que stratégiquement cela l'était, « *La sécurité et la confidentialité des données personnelles est dans notre ADN, s'il n'y a pas de respect des données de nos clients, on a pas de business.* »

C'est une véritable valeur ajoutée. Les données privées sont critiques pour tous nos clients mais selon leur secteur d'activité, nos contrats variaient en fonction des niveaux d'exigence propres à chaque client. La conformité avec le RGPD permet d'aligner les exigences de l'ensemble de nos clients sur une norme acceptée et comprise par tous. Cela nous permet de concentrer nos efforts sur la mise en oeuvre d'une infrastructure respectant la norme qui rassure et simplifie la vie de tout le monde.

— Charles Dunston, CEO, Dial Once

Publication : juin 2018

Le DPO, le garant de la conformité RGPD

Il y a essentiellement deux raisons qui vont déclencher les révisions des politiques de sécurité et des traitements. La première est naturellement le changement des réglementations. [...] La seconde raison est tout simplement la modification de traitements...

— Yves Gattegno, DPO, Dial Once

Yves Gattegno arrive chez Dial Once comme CDO, Chief Data Officer, un titre important au sein d'une société où la confidentialité des données est au coeur de tous les traitements.

Aujourd'hui avec la mise en pratique du RGPD depuis le 25 mai 2018, le rôle d'Yves Gattegno a naturellement évolué vers celui de DPO, Data Privacy Officer. Il est officiellement nommé à ce poste au sein de Dial Once et est également déclaré auprès de la CNIL. Au départ c'est un homme de la technique, ingénieur informaticien puis un startuper ce qui le pousse à s'intéresser au droit. Une expérience apprise sur le terrain avec la lecture du code de propriété intellectuel, puis celui de la consommation, ce qui le plonge dans les arcanes des contrats, pour étudier enfin le règlement général sur la protection des données.

À chaque traitement de données personnelles, des obligations

« *Avec le RGPD, ce qui a vraiment changé c'est qu'il existe un cadre juridique très précis et l'obligation de rendre compte. Je dois m'assurer que la société est constamment conforme au RGPD. Je surveille les relations avec nos partenaires, sous-traitants ou clients. Tout particulièrement au moment de la négociation d'un contrat commercial, il faut analyser de près les dispositions sur la protection des données personnelles. Je produis dans ce cadre de la documentation plus externe qu'interne car elle sera essentiellement destinée à l'usage de nos clients et partenaires afin de leur expliquer ce que nous faisons en termes de données à caractère personnel : ce que l'on collecte, ce que l'on traite, comment on s'assure de la sécurité, de la confidentialité, de la disponibilité de ces données. Les documents produits évoluent naturellement en même temps que les traitements dans le temps.* » explique Yves Gattegno.

Dial Once travaille avec de grands groupes internationaux ce qui fait du DPO le Responsable chargé de répondre aux questionnaires des clients qui ont d'ores et déjà des procédures internes instaurées (banque, assurance ...). Des questionnaires qui s'assurent que le sous-traitant respecte bien les normes en termes de sécurité des données personnelles. Suit généralement des entrevues avec les responsables de la sécurité et/ou de la confidentialité chez les partenaires pour aller plus en détail sur les procédures réalisées.

Quand évolution des traitements rime avec conformité dans le temps

De temps en temps, la politique de confidentialité est révisée sous l'impulsion du DPO puis les corrections validées en comité de Direction. « *Il y a essentiellement deux raisons qui vont déclencher les révisions des politiques de sécurité et des traitements. La première est naturellement le changement des réglementations. Ainsi avec le RGPD, on a beaucoup plus d'informations à fournir comme par exemple,*

l'apparition officielle du DPO au sein des mentions légales. La seconde raison est tout simplement la modification de traitements, par exemple traiter une donnée différemment ou ne plus la traiter... » précise yves Gattegno.

Le DPO : à cheval entre le juridique et la technique

L'arrivée de la RGPD en France n'a pas fondamentalement changé grand chose par rapport au nombre de lois auxquelles étaient déjà soumises les entreprises (Loi Informatique et Libertés de 78, loi pour une république numérique ...) selon le DPO de Dial Once. L'esprit des réglementations reste le même alors que les sanctions deviennent beaucoup plus importantes ce qui change de beaucoup la donne par rapport aux amendes imposées jusqu'à présent. C'est dans ce contexte que le DPO a la charge de vérifier que l'entreprise est bien en conformité avec la réglementation et pour cela, il y a deux aspects à prendre en compte, l'aspect juridique du RGPD relatif au réglementaire et celui opérationnel c'est-à-dire vérifier que le traitement mis en œuvre techniquement est bien en accord avec la réglementation.

Savoir travailler avec l'Opérationnel

Il faut s'assurer que les choix technologiques réalisés par la DSI n'empêche pas dans le temps à l'entreprise de rester conforme au RGPD. Par conséquent le DPO interagit avec les équipes techniques afin de s'assurer que la mise en œuvre soit bien pensée en amont afin qu'elle ne vienne pas dans le temps mettre en péril la conformité au RGPD de l'entreprise. Il doit s'assurer qu'elle évolue tout en restant conforme aux législations en cours.

Il existe des outils dont certains mis à disposition par la CNIL notamment un open source pour réaliser des analyses d'impacts. Il aide le DPO à poser les bonnes questions aux équipes opérationnelles. « *Le fait de répondre à 80% des questions posées permet de faire 80% du travail. Cependant lorsque le DPO est issu d'un milieu purement juridique, il se peut qu'il existe quelques incompréhensions difficiles à lever entre lui et les équipes techniques. L'échange peut prendre un plus de temps...* »

Le fait de répondre à 80% des questions posées permet de faire 80% du travail. Cependant lorsque le DPO est issu d'un milieu purement juridique, il se peut qu'il existe quelques incompréhensions difficiles à lever entre lui et les équipes techniques. L'échange peut prendre un peu plus de temps ...

— Yves Gattegno, DPO, Dial Once

Publication : juin 2018

Conformité RGPD : savoir coupler une solution mature aux développements internes

En déléguant en partie les problématiques de sécurité, de chiffrage et de maintenance à un spécialiste des données, nous pouvons nous concentrer sur notre métier. C'est un élément crucial pour notre développement.'

— Julien Kernec'h, CTO, Dial Once

Chez Dial Once, le passage au RGPD a presque été une formalité

« La société a 4 ans d'existence. 4 ans que nous travaillons avec des données personnelles et renforçons sans cesse la sécurité de nos plateformes. La majorité de nos clients proviennent du secteur de la banque et de l'assurance qui sont très sensibles sur le sujet des données personnelles. C'est donc à la demande de ces clients que nous avons intégré des fonctions spécifiques en plus de celles qui nous semblaient nécessaires d'un point de vue sécurité opérationnelle. Avec l'imminence du RGPD, nous avons dû intensifier nos efforts. S'il fallait engager un tel processus aujourd'hui en partant de rien, l'effort serait considérable tant pour s'assurer que les données sont stockées proprement, les pseudonymiser voire les anonymiser ou les chiffrer en fonction des cas. »

Audits & Bug Bounty pour éprouver la solidité

Lors du lancement de l'entreprise, la mise en place de cette infrastructure sécurisée a nécessité de nombreux échanges avec des prestataires externes, sociétés de conseils et d'audit de plateforme. Un travail qui aura duré deux ans pour identifier les données, définir des actions précises et les mettre en place.

Aujourd'hui encore un point mensuel est réalisé pour analyser les résultats des audits sécurité de la plateforme Dial Once ou de façon ponctuelle à la demande de nos clients. Le DPO de Dial Once est sollicité dans ce processus afin de valider la conformité au RGPD à chaque modification de traitement.

Enfin, Dial Once engage également des campagnes de Bug Bounty par l'intermédiaire d'une plateforme spécialisée. Un Bug Bounty est un programme proposé par de nombreux sites web et développeurs de logiciel qui permet à des personnes de recevoir une reconnaissance et une compensation après avoir reporté des bugs, surtout ceux concernant des exploits et des vulnérabilités, celles-ci sont chargées de coordonner le travail de hackers indépendants rémunérés en fonction de leurs découvertes de failles ou de vulnérabilités.

Traiter les bonnes données & Sécuriser la connexion

A l'occasion de nouveaux traitements, s'il subsiste le moindre doute sur le type de données traitées, des recherches sont alors effectuées pour lever toute ambiguïté. Pour cela, le CTO n'hésite pas à rencontrer les services juridiques de ses clients pour clarifier la typologie de la donnée et décider de la façon dont elles devraient être traitées :

- Soit dans les Datacenters Dial Once sur des serveurs avec du chiffrement symétrique ou asymétrique selon le degré de criticité de la donnée
- Soit envoyées directement chez le client, le flux de données ne faisant que transiter via les serveurs Dial Once pour assurer leur transmission.

Notons que toutes les connexions au service (entre utilisateurs et serveurs) sont sécurisées. Et bien souvent, le flux est même pré-chiffré côté utilisateur.

Respecter les droits d'accès aux données

Au-delà de ces précautions, d'un point de vue opérationnel, il reste encore la question de la répartition des responsabilités de chaque employé de Dial Once dans le but de savoir qui a le droit d'accéder aux données. Cette ségrégation implique des contraintes opérationnelles certaines.

Savoir s'appuyer sur l'existant mature

Pour Dial Once, traiter ce genre de problème en interne en développant sa propre solution est très coûteux tant en ressources qu'en moyens et en temps, car il faut intégrer de nouvelles fonctions qui complexifient d'autant le traitement des données (chiffrer, anonymiser, pseudonymiser, répartir les accès ...). C'est en participant au programme « Oracle Startup Cloud Accelerator » que Julien Kernec'h, CTO de Dial Once, est accompagné pour prendre connaissance des derniers services proposés sur la base de données Oracle. Des services récemment mis à jour pour être spécifiquement conformes au RGPD et résoudre les contraintes opérationnelles. Notamment des options pour pouvoir chiffrer les données ou les masquer par rapport à des rôles ou des permissions en fonction des droits d'accès des employés, auditer les données, procéder à des extractions et récupérer des données sans le faire manuellement.

Julien Kernec'h explique : « *Il vaut mieux utiliser une solution mature et spécialisée afin de concentrer nos compétences internes sur les développements du produit et particulièrement quand on est une start-up. Réaliser en interne ce type de développement est extrêmement lourd, cela aurait impacté notre chiffre d'affaires, car nous n'aurions pas concentré nos efforts à améliorer notre produit et proposer de nouvelles offres à nos clients. Enfin, le service Oracle est proposé en standard « on premise » comme dans le Cloud, ce qui correspond aux contraintes de notre plateforme.* » *Et Hakim Loumi, expert GDPR Oracle, renchérit : « On peut estimer qu'aujourd'hui, à 95%, la gamme des produits Oracle est conçue pour répondre aux exigences GDPR et ce, en ne considérant que la partie technologique (anonymisation, chiffrement, pseudonymisation, datanomisation, gestion des identités et des accès, sécurisation des données, gouvernance ...).* »

Les données au cœur du problème

Il existe donc aujourd'hui plusieurs opérations à appliquer sur les jeux de données pour les rendre partiels tout en gardant leur cohérence et leur pertinence (datanomisation), pour les masquer (anonymisation), pour les rendre anonymes sans

En déléguant en partie les problématiques de sécurité, de chiffrage et de maintenance à un spécialiste des données, nous pouvons nous concentrer sur notre métier. C'est un élément crucial pour notre développement.'

— Julien Kernec'h, CTO, Dial Once

espoir de retour aux données originales (anonymisation statique) ou de façon ponctuelle (anonymisation dynamique). Dans ce dernier cas, on ne masque pas la donnée dans la base ou dans le fichier, voire sur le disque dur, mais seulement à l'affichage, au moment où elle est rendue visible à l'utilisateur, on y applique simplement un filtre de masquage. La donnée reste toujours la même et n'apparaîtra qu'en fonction d'une habilitation. L'anonymisation dynamique est également une pseudonimisation. Dans certains cas, la pseudonymisation correspond à un éclatement de la donnée que seul un algorithme intelligent peut reconstituer. Autant d'options à sélectionner dans les outils Oracle.

Anonymiser ou Masquer la donnée ?

Cet éventail d'options sur les données proposé au sein des services Oracle est important dans le contexte du RGPD pour une entreprise car, grâce au « Considérant 26 », toutes données anonymisées ne sont plus soumises à la conformité RGPD et à son lot de contraintes. Dans toute entreprise, beaucoup de données ne sont soumises à aucun traitement. Les anonymiser via une option disponible via un service Oracle serait donc une solu-

tion rapide et efficace pour ne pas alourdir inutilement les processus RGPD à mettre en œuvre. Ne reste qu'à choisir les options qui conviendraient le mieux à leur schéma de traitement de données pour celles qui sont encore à traiter et ainsi répondre aux exigences du Règlement Général (masquage dynamique, chiffrement, audit ...).

SGBD (Système de Gestion de Base de Données) pour RGPD : CQFD ...

Cette facilité d'action permettrait à de nombreuses entreprises qui ont cumulé des Téraoctets de données dans leurs bases de ne pas avoir à refondre complètement leur Business Model dans des laps de temps souvent très courts et sans les bonnes compétences en interne ... La tendance revient donc à choisir des bases de données qui intègrent les fonctions nécessaires pour sécuriser les données, des fonctions de préférence codées au niveau du noyau pour ne pas impacter les performances de fonctionnement de ladite base. « *Souvent, ces bases de données (comme Oracle, SQL Server ou DB2) ont des renommées et cette image de marque est également un atout auprès des clients. Jusqu'à présent, nous avions développé au niveau applicatif et en nous appuyant sur une base de données non sécurisée. Nous avons donc migré vers Oracle. Une solution qui devient également intéressante, car nos besoins métiers évoluent (différents niveaux de droits d'accès, possibilité d'accès aux données personnelles via un portail pour la gestion du droit à l'oubli, faire des audits ...). Au final, même s'il y a un certain coût, c'est un bon choix à faire. En déléguant en partie les problématiques de sécurité, de chiffrage et de maintenance à un spécialiste des données, nous pouvons nous concentrer sur notre métier. C'est un élément crucial pour notre développement.* »

Publication : juin 2018