A N D S I

Association Nationale des Directeurs des Systèmes d'Information
www.andsi.fr

Le projet RGPD chez Econocom

Compte rendu de la présentation du 14 novembre 2017, aux Foudres de Bacchus.

Compte rendu rédigé par Laure MUSELLI & ANDSI

En bref…

Charles DELATTRE et Christophe MERCKENS, respectivement RSSI et DSI du groupe Econocom, présentent l'avancement du projet de mise en conformité au Règlement Général sur la Protection des Données (RGPD) mené au sein de leur entreprise. Après un rappel des grands objectifs du RGPD qui entrera en vigueur le 25 mai 2018, ils exposent les différentes étapes du plan d'action d'Econocom pour la mise en conformité au RGPD. Ils listent enfin un certain nombre de points d'attention à ne pas négliger pour réussir sa mise en conformité.

Econocom est groupe de services européen qui compte un peu plus de 10 000 collaborateurs, est présent dans 19 pays et réalise 2,5 milliards d'euros de chiffre d'affaires. L'entreprise possède trois métiers historiques qui sont la distribution d'équipement (PC, tablettes, routeurs, etc…), le financement (leasing) et le service, suite au rachat de la société Osiatis en 2014, selon un modèle original de bundle comprenant par exemple un smartphone, le développement d'une application dédiée, le service et la maintenance en leasing sur 3 ans.

Le groupe est construit sur un modèle de « planète » comprenant 8 000 collaborateurs, et de filiales « satellites » récentes (2 000 collaborateurs), qui gardent leur identité en termes de fonctionnement et sont positionnées sur des métiers spécifiques comme du cloud, de l'IoT, de la cybersécurité ou encore du conseil en management.

La mise en conformité au RGPD a été abordée par Econocom comme une obligation suscitant des craintes, et qu'il a fallu prendre en charge de façon pragmatique. Aujourd'hui, l'entreprise, si elle n'est pas totalement conforme, a mis un plan d'action en œuvre et est confiante sur cette question.

Retour sur le RGPD

Le RGPD sera applicable à partir du 25 mai 2018 à toute entreprise européenne, mais aussi à toute entreprise traitant des données à caractère personnel de citoyens européens.
Il comporte trois objectifs :

- Renforcer le droit des personnes en créant de nouveaux droits
- Responsabiliser les acteurs traitant des données (responsables de traitements et sous-traitants, avec une notion de co-responsabilité et de responsabilité descendante)
- Crédibiliser la régulation : celle-ci devient homogène sur l'ensemble de l'Europe et l'amende maximale passe de 150 000 euros (payés pour la première fois par Google et représentant le bénéfice réalisé par l'entreprise en 8 secondes) à un maximum de 4% du CA du groupe en cas d'incident, pouvant être ramené à 2% si des efforts de sécurité sont démontrés.

Le plan d'action d'Econocom

Ce plan d'action a été développé en capitalisant sur les bonnes pratiques mises en ligne par la CNIL sur son site et sur les 6 piliers qu'elle identifie pour mettre une organisation en conformité.

1- Piloter la mise en conformité

En phase projet, c'est la direction juridique qui gère le pilotage.

- La société s'est dotée d'une **AMOA** du chantier de la mise en conformité auprès de Digital Security, une entité satellite d'Econocom spécialisée sur ces questions, ainsi que d'une **prestation d'assistance** auprès d'une société externe.
- Du projet doit émerger un **livrable incontournable : la Politique de Protection des Données**, qui montre l'engagement de l'entreprise et doit pouvoir être communiquée à toute personne impliquée dans une opération de traitement de données personnelles. Elle doit indiquer les grandes lignes de la politique de l'entreprise et mentionner les moyens à mettre en œuvre et tous les éléments d'entrée nécessaires à la tenue du registre des traitements auditable par la CNIL : qui sont les responsables, quelles sont les données traitées, les finalités de traitement, qui s'en charge, qui sont les sous-traitants, qui sont les accédants (par exemple, on peut s'engager à ce que les données ne sortent pas de l'Union Européenne, à ce que les accédants ne soient que des salariés de l'entreprise, etc…).

En run, le rôle de DPO est attribué à une juriste spécialisée de la protection des données
Le principe est celui d'un guichet unique permettant de :

- Contrôler le respect du règlement,
- Conseiller sur la réalisation d'études d'impact concernant la protection des données et d'en vérifier l'exécution,
- Coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Elle devrait être rattachée à la direction juridique et reporter à un haut niveau au sein de l'entreprise, conformément au Règlement.

2- Cartographier les données à caractère personnel

Le règlement impose une **obligation de documentation interne complète** des traitements de données à caractère personnel recensant :

- Les différents traitements de données à caractère personnel,
- Les catégories de données personnelles traitées,
- Les objectifs poursuivis (les finalités),
- Les acteurs (internes ou externes) qui traitent ces données,
- Les flux en indiquant l'origine et la destination des données.

.
Un **modèle de registre fourni par la CNIL** comporte notamment un onglet intéressant recensant les pays en conformité avec le RGPD et dans lesquels il est possible de stocker des données, et ceux qui ne sont pas dotés d'une réglementation adéquate. Le fait d'exporter des données dans un pays non-adéquat fait d'ailleurs partie des critères de demande d'avis préalable à la CNIL.

Globalement, il s'agit de répondre aux questions : **Qui ? Quoi ? Pourquoi ? Où ? Jusqu'à quand** (car la donnée à caractère personnel ne peut être gardée indéfiniment)**? Comment** (spécification des sous-traitants, qui, si eux-mêmes sous-traitent, doivent obtenir l'aval du responsable amont)**?**

Chez Econocom, le groupe ayant beaucoup grossi par croissance externe et rachats, le démarrage s'est fait « from scratch », avec un premier inventaire des traitements déclarés à la CNIL qui a servi de base de travail.
La première étape a donc été cet inventaire des traitements. Sur le site internet de la CNIL, il est possible d'effectuer une recherche de l'ensemble des données à caractère personnel (DCP) déclarées par l'entité juridique. Une capitalisation a été effectuée sur ce premier inventaire pour avoir une première évaluation de la conformité au RGPD.
Si le site de la CNIL permet une vue de base et un point de départ complet, les déclarations ne sont pas à 100% conformes avec le RGPD. Par ailleurs, lorsqu'une société rachète environ dix entreprises par an, il est difficile de savoir quelles sont les déclarations qui ont été faites dans une filiale acquise il y a quelques mois, voire dans ses sous-filiales.

3- Prioriser les chantiers

En termes de périmètre, c'est celui de la France qui a été priorisé, car il s'agit, pour l'entreprise, du périmètre commercial le plus important (65% de l'activité). L'IT étant traité en France, la majorité des traitements de données à caractère personnel (90%) se situe également en France.

En termes de métiers, parmi les activités d'Econocom (leasing, distribution, service), c'est l'activité de service qui a été priorisée. Il existe en effet un peu moins de pression de la part des clients pour les autres activités : lorsqu'ils donnent les clés de leur IT et de leurs données personnelles, ils sont plus regardants que lors d'une simple fourniture de matériel.

En termes de nature de donnée traitée, plus la donnée est sensible, plus elle est prioritaire : on ne traite pas un RIB comme une fiche de paye ou comme un numéro de matricule.

L'entreprise se pose encore quelques questions en ce qui concerne ses filiales « satellites ». Pour ceux dont elle est détenteur à 100% ou actionnaire majoritaire, Econocom risque une amende de 4% du chiffre d'affaires du groupe en cas de problème. En revanche, pour les satellites dans lesquels le degré de participation de l'entreprise est faible, une étude juridique est en cours pour évaluer s'ils sont considérés comme faisant partie du groupe et quelle serait la responsabilité d'Econocom en cas de problème.

4- Gérer les risques

Les analyses de risques sont obligatoires dans le nouveau règlement, alors qu'elles étaient seulement recommandées auparavant.
Elles sont appelées **PIA (privacy impact assessment)** et sont des analyses de risques de type sécurité des informations, plus particulièrement axées sur la protection des données à caractère personnel.
En cas d'incident, le **PIA est un élément fondamental** pour démontrer à la CNIL le respect du règlement. La CNIL demandera l'analyse de risques réalisée, afin d'apprécier le niveau de prise en compte des risques et surtout la pertinence des mesures prévues et mises en œuvre pour les limiter (mesures proportionnées au type de risque et à la criticité de la donnée).
Un outil, qui adopte l'approche ISO27005 EBIOS centrée sur le risk management et permettant de décliner cette analyse de risques est disponible sur le site de la CNIL. Il peut constituer un bon guide pour débuter dans cet exercice, car il récapitule les évènements redoutés, les sources de menaces, les échelles d'impact, etc…

Trois critères principaux sont à évaluer : **l'accès illégitime** aux DCP, **la modification non-désirée** des DCP, **la disparition** des DCP.
Par rapport à chacun des risques, il faudra : soit **diminuer le risque d'occurrence** (par exemple en changeant les modalités d'accès à la donnée), soit en **diminuer l'impact** (par exemple en chiffrant les données susceptibles d'être volées).
En cas de problème, l'enjeu se situe dans un montant d'amende qui peut passer de 4% à 2% du chiffre d'affaires !

Econocom a capitalisé sur un grand nombre d'analyses de risques déjà réalisées dans le cadre de sa certification 27 001, qui rend l'analyse de risques obligatoire, et les a adapté au sujet des DCP.
L'outil utilisé est Risk'n TIC, qui permet de réaliser de la sécurité d'information en intégrant un référentiel protection des DCP.

5- Organiser les processus internes en anticipant les nouvelles obligations légales

Alors que le RSSI arrive bien souvent en dernier ressort, l'idée consiste à renverser cette logique en se plaçant très en amont des projets, pour intégrer la problématique de protection des DCP dès le départ, comme cela avait déjà été réalisé pour la sécurité de l'information.

Le **degré de sensibilité du projet est évalué** grâce à un **questionnaire en amont** pour :
- Prévenir des potentiels risques sur les DCP
- Prévoir le recueil du consentement si nécessaire

De manière générale, le « by design » est plus facile à mettre en œuvre que la « rustine ».

Des **actions de sensibilisation/formation des collaborateurs à la protection des DCP sont obligatoires** et ont été mises en place dans le cadre d'un plan de communication, en capitalisant sur les mesures et les outils mis en œuvre pour la certification ISO 27 001. L'outil utilisé est un module vendu par Karspersky.

Le **traitement des réclamations et demandes** était une notion déjà existante, mais qui a été beaucoup renforcée avec le RGPD :
- droit d'accès,
- droit de rectification,
- droit d'opposition,
- droit à la portabilité, y compris de la part des fournisseurs, sous forme intelligible, de façon à pouvoir en faire un autre usage
- droit de retrait du consentement, obligation de demande de consentement préalable au traitement des DCP. Par exemple, un consentement préalable est demandé aux employés pour introduire leurs données personnelles dans un logiciel de paie, ceux-ci devant également être informés du type de traitement qui sera fait de leurs données. Pour les salariés, il est conseillé de recueillir ce consentement dans le cadre du contrat de travail. Il faut également être capable d'effacer les données traitées en cas de retrait du consentement.

L'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen

Les violations de données doivent être notifiées à la CNIL dans les 72h, sauf justification. Dans certains cas, les personnes doivent également directement être notifiées dans les meilleurs délais, ce qui nécessite de posséder les informations nécessaires pour les contacter. Lorsque l'on est capable de montrer que l'impact était faible et que les mesures ont été prises pour éviter le vol de données, une déclaration publique (sur la page d'accueil par exemple) peut être suffisante.

6- Documenter dans un souci d'auditabilité et de preuve en cas de contrôle.

Les **documents attendus** par les autorités de contrôle concernant les traitements sont :
- Le registre des traitements
- Les PIA
- Les contrats ou cadres régissant les éventuels transferts hors UE. Il existe sur le site de la CNIL des clauses contractuelles standard, de fait en accord avec la réglementation. Par ailleurs, les transferts hors UE nécessitent également le recueil du consentement

En ce qui concerne le **droit d'information des personnes**, il faut pouvoir présenter :
- Les mentions d'information
- Les modèles de consentement des personnes
- Les procédures de mise en œuvre des droits des personnes (avec procédures documentées, indiquant les rôles et responsabilités des acteurs de la chaîne)

En ce qui concerne **les rôles et responsabilités**, il faut pouvoir produire :
- Les contrats de sous-traitance (obligations des sous-traitants et contrôle des mesures de protection, car co-responsabilité)
- Les procédures de gestion de crise en cas de violation des DCP
- Les preuves de consentement

Les principaux points d'attention

- Ne collecter que le strict nécessaire
- Prendre en compte les éventuelles autres bases juridiques applicables au traitement (c'est-à-dire les autres législations qui s'appliquent à certaines données comme les données de santé).
- Respecter le consentement préalable à tout traitement (sauf quelques traitements concernant les casiers judiciaires ou les contraventions, qui sont exemptés de consentement préalable)
- Réviser régulièrement les documentations
- Mettre en place un suivi des sous-traitants et des contrats. Il s'agit d'un point dur, comme en témoigne la condamnation d'un opérateur Télécom pour défaut de sous-traitance, qui a conduit à la mise en place d'une politique drastique de suivi de ses sous-traitants
- Bien anticiper l'exercice des droits des personnes
- Contrôler régulièrement les mesures de sécurité (ce qui doit pouvoir être démontré en cas d'incident)

Conclusion :

La plupart des fondements du règlement étaient déjà présent dans la loi de 1978, les changements tenant plutôt à l'harmonisation au niveau européen et au montant des sanctions. Le RGPD fait ressortir quatre sujets importants :
- L'importance du consentement préalable
- Le renforcement du droit des personnes
- Une notion de co-responsabilité qui n'est pas anodine
- L'anticipation des incidents, en démontrant leur prise en compte en amont, afin d'éviter de lourdes sanctions

Le processus s'inscrit dans une démarche d'amélioration continue conforme à ce qui peut exister dans le référentiel général de sécurité des administrations publiques par exemple, avec une notion d'homologation des systèmes d'information, d'analyse de risques et d'appréciation des risques individuels.

Pour les autorités de contrôle, **le 25 mai n'est pas une date butoir** : aujourd'hui, il existe une quinzaine d'inspecteurs prêts et formés, qui ne pourront pas contrôler l'ensemble des entreprises. **L'essentiel est d'avoir pris le sujet en amont, d'avoir défini un plan d'action et commencé à le mettre en œuvre**. Il reste encore un peu de temps pour terminer de se préparer à condition de pouvoir démontrer que le projet a été démarré et avance.
Par ailleurs, il existera très bientôt une offre de certifications RGPD *compliant*, même si aucune n'est encore homologuée par la CNIL.

Débat

Intervenant : Tout n'est pas sur le site de la CNIL ! La tenue du registre de CIL n'apparaît pas sur le site de la CNIL. Il manque un certain nombre de choses. Lorsque l'on a un CIL interne, on n'a pas toutes les notions de tenue de registre, mais seulement les déclarations volontaires. Par exemple, j'ai un CIL interne qui tient son registre de traitements, dont les informations ne sont pas visibles sur le site de la CNIL.
Charles DELATTRE : Exactement. Et inversement, il existe une autre coquille, car à force de rachat, lorsque nous avons voulu déclarer un traitement au nom d'une entité juridique, la CNIL a répondu que nous avions déjà un CIL. Lorsque le CIL est parti, nous avons perdu ses registres et sa connaissance avec lui.

Int. : Quelles sont les options possibles en cas de filiale satellite un peu « en dehors des clous » ?
C. D. : La mettre dans les clous ! La stratégie peut consister à décentraliser en nommant un DPO pour ce satellite particulier, afin de se décharger d'un certain niveau de responsabilité, ou à l'inverse, à lui appliquer les process du groupe.

Int. : Qu'en est-il des historiques à garder dans les archives, comme en ce qui concerne l'archivage obligatoire des bulletins de paie ? Et quid des sauvegardes ?
C. D. : Il existe deux notions : la pseudonymisation ou l'anonymisation des données (détruire la correspondance matricule, avec un identifiant unique qui ne soit plus rattaché à une personne physique). Par ailleurs, cette obligation ne se substitue pas à d'autres obligations légales : si une autre loi impose de garder les données, comme des bulletins de paie, on peut les garder. Il va également être compliqué de supprimer les sauvegardes, mais pour éviter tout problème, il faut les chiffrer en amont, de façon à ce qu'en cas de fuite, on ne puisse pas savoir ce qu'il y a dans les données.

Int. : Qu'advient-il des autorisations CNIL actuelles ?
C. D. : Les traitements déclarés devront tout simplement être reportés dans votre registre. Il faut plutôt favoriser les déclarations cadres dans les registres. Ne déclarez pas par application, mais par finalité de traitement. Quand on rachète dix entreprises et qu'il y a dix logiciels de paie, il s'agit d'une seule finalité de traitement, donc une seule ligne dans le registre (s'il s'agit des mêmes accédants, mêmes données traitées, mêmes finalités de stockage, etc…). Il faut privilégier la mutualisation des déclarations et entrées dans le registre.

Int. : En cas d'incident, la forme de la notification (globale ou personnelle) aux personnes dépend-elle du type et de la sensibilité de la donnée ?
C. D. : Il existe une notion de sensibilité dans le règlement, mais il n'y a pas de définition précise de cette sensibilité : c'est la jurisprudence qui définira cela plus précisément. On n'a pas de recul sur ce qui est sensible ou pas, mais c'est prévu.

Int. : En termes d'homologation, le Cabinet Bensoussan et le Bureau Veritas se sont associés pour créer une « certification » : cela peut-il aider un cabinet d'avocats à plaider pour réduire les conséquences financières en cas de poursuites ?
C. D. : Je ne suis pas au courant, mais ce doit être un label qui constitue une sorte de contrôle externe.

Int. : Comment avez-vous pris en compte les progiciels et les données personnelles qu'ils traitent ? Avez-vous reporté la responsabilité sur l'éditeur ?
C. D. : On ne peut pas reporter la responsabilité sur lui, sauf s'il est sous-traitant à part entière (c'est-à-dire hébergeurs) En SaaS, en revanche, ils sont sous-traitants. C'est plutôt en phase amont, la direction juridique et moi-même, qui devons anticiper, à l'occasion d'une révision de contrat ou dans le cadre d'un nouveau contrat, les conditions de la conformité. A défaut d'une politique de protection des données, nous avançons sur la base d'un modèle de plan d'assurance sécurité, c'est-à-dire que l'on s'assure qu'ils ont mis en place ou qu'ils vont mettre en place un certain nombre de protections au sein de leur système d'information et l'éventuelle capacité de chiffrement de certains champs du logiciel relatifs au traitement de données à caractère personnel, sans que cela nous soit facturé. Pour les choses plus anciennes, c'est un peu d'archéologie et la connaissance de chacun du logiciel : nous connaissons assez bien les champs.

Int. : La maréchaussée est quasi-inexistante, avec 15 inspecteurs, ce qui est rien pour 2 millions d'entreprises. C'est donc une loi contre les Américains. Est-ce que la loi est raisonnablement applicable (si on cherche à évaluer le risque) ? On peut évaluer le risque en fonction du coût et faire ou ne pas faire. C'est un bon prétexte pour toutes les boîtes de conseil pour vendre des consultants, comme pour le passage en l'an 2000. Est-ce applicable et a-t-on des chances de se faire prendre ?
C. D. : Je pense que oui, c'est applicable, car le problème n'est pas le contrôle, le radar. Le problème surgit lorsque l'accident arrive. Et les accidents sont plutôt en hausse. Le risque de se faire prendre dans un contrôle est très faible, car les autorités vont tout d'abord cibler les GAFAs, les très grosses entreprises et celles qui traitent de la donnée très sensible, comme dans le médical. Ma crainte n'est pas celle du contrôle, mais celle de la fuite et du piratage. C'est à ce moment-là que la CNIL va sanctionner. Si le risque de contrôle est plutôt faible, le risque de piratage est en augmentation et l'impact de plus en plus important.

Int. : Si on parle d'accident, existe-t-il des contrats d'assurances ?
C. D. : Oui ! Et pour pouvoir être bien assuré, il faudra faire tout ça, car les assureurs ne prendront pas de risque non plus ! Il existe des assurances sur les données personnelles et plus largement sur la sécurité de l'information. Mais les assureurs font un audit préalable.

Int. : Dans votre cas, lorsque l'on parle de consentement, on parle plutôt de salariés. Mais pour toutes les entreprises qui gèrent aussi les données de prospects et de clients, comment se passe le consentement des clients ?
C. D. : Par rapport aux clients, notre métier étant de développer des applications, nous formons nos collaborateurs à la notion d'obligation de consentement, pour que ce volet soit prévu dans les applications développées.

Int. : Et lorsque l'on collecte des informations par téléphone, est-ce qu'il faut demander son consentement au client, ou est-ce que cela est valable seulement pour les sites web ?
C. D. : Ca va aller jusque-là, à partir du moment où on collecte de la donnée personnelle. Dans les centres d'appel, on précise déjà que l'appel peut être enregistré, et on peut pousser jusqu'à dire qu'en continuant la conversation, on consent à ce que le nom, prénom, etc, soient enregistrés.

Int. : Et il faudra être capable de communiquer toutes ses données au client ?
C. D. : Il va falloir être en capacité, lorsque la personne demande les données la concernant, de les lui fournir. C'est le fameux droit d'accès. Une utilisatrice a demandé à Twitter ses données personnelles et ils lui ont fourni 800 pages.

Présentation des orateurs

Charles DELATTRE est RSSI du groupe Econocom :

- Bac +5 en Architecture et management des SI. Avec un passé de RSSI des Services Judiciaires au Ministère de la Justice et d'ingénieur sécurité à l'ANSSI/CERT-FR

Christophe MERCKENS est DSI du groupe Econocom :

- Double formation IT & Finance

- 30 ans de carrière dans le domaine de l'IT, depuis 15 ans sur des postes de grands projets ou de transformation dans des groupes internationaux