Marie-Noëlle Gibon
Correspondant Informatique et Libertés
Groupe La Poste

Eléments de contexte

La Poste, en tant que responsable de traitement, a la responsabilité de 10 millions de comptes de particuliers. En tant que sous-traitant, elle gère cinq milliards d'événements colis et 70 milliards d'événements courrier par an. La question de la protection des données personnelles est donc, pour cette entreprise, un enjeu majeur.

La conformité peut être assimilée à une recette de cuisine faisant intervenir trois ingrédients principaux : des individus (devant être dotés des compétences nécessaires), des projets à piloter, enfin une boîte à outils pour construire la conformité.

Garantir la conformité et la sécurité des données : les chantiers à conduire

Les premières actions mises en place concernent la tête du Groupe : le Comex qui, en mars 2016, a été initié aux principes clés du Règlement sur la protection des données. Il a en outre validé six chantiers, dont il va être question ci-dessous. Le Correspondant Informatique et Libertés (CIL) en sera le pilote pour aider chacun à franchir les obstacles sur le chemin qui conduit à la conformité aux obligations contenues dans le Règlement. Il faut rappeler que le CIL est rattaché directement à un membre du Comex et, de fait, n'est pas sujet aux conflits d'intérêt mis d'ailleurs en exergue par le Règlement sur les fonctions du Délégué à la protection des données (DPO).

Analyser l'existant

Il s'agit d'identifier toutes les actions d'ores et déjà mises en œuvre pour respecter les obligations en vigueur – et d'en évaluer le coût.

Evaluer l'impact des différentes mesures induites par le Règlement sur les activités du Groupe

L'impact porte sur l'organisation, les processus, les SI. Il a été demandé aux activités bancaires, d'une part, et aux autres activités, d'autre part, d'examiner les chapitres 3 et 4 du Règlement (droit des personnes, obligations de l'entreprise). Sur une échelle de zéro à cinq, elles ont dû évaluer l'impact de ces dispositions afin d'identifier les actions à mettre en œuvre, dans une logique de priorisation. Cet impact, comme dit précédemment, est à évaluer sur l'organisation, les processus et les SI.

Sur cette base, un schéma d'ensemble de la mise en conformité a pu être établi. Chantier par chantier, lot par lot, des structures projet vont être définies et les opérations lancées. La revue des registres existants sera probablement l'opération la plus simple à mener, compte tenu du temps restant (deux ans). Ce temps sera en revanche beaucoup plus contraint sur, par exemple, les actions à mettre en œuvre en matière de sécurité.

Pour chaque chantier, chaque tâche, des calendriers ont été établis.

Valoriser les options possibles

Les actions à mettre en œuvre doivent être priorisées, leur coût évalué. Des budgets doivent naturellement accompagner chaque action… ce qui n'a rien de simple, dans la mesure où de nombreuses inconnues demeurent. Il faudra probablement, de facto, constituer des provisions.

Mettre en œuvre et piloter les projets

Ces projets devront naturellement être mis en œuvre avant le 25 mai 2018. A noter dans ce cadre qu'il faudra réviser toute la documentation contractuelle, ce qui générera une charge de travail conséquente. Il faudra, aussi, réviser les contrats de prestation, dans la mesure où de nouveaux points, conséquences directes du Règlement, devront être pris en considération.

L'article 34 du Règlement pose que « le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ». Certaines actions (sur l'analyse de risque par exemple) ont d'ores et déjà été lancées – dans certains métiers, la banque en particulier, l'analyse de risque est automatiquement menée pour tout projet. Au-delà, il faudra :

- Intégrer ses propres exigences de sécurité dans le cahier des charges ;
- Rédiger les clauses contractuelles afférentes à la sécurité ;
- Elaborer un Plan d'Assurance Sécurité conjointement avec le prestataire ;
- Tester les plans de réversibilité – il faut être en mesure de récupérer les données qui ont été confiées à un prestataire. Il s'agit d'une question centrale dans la mesure où, les technologies évoluant rapidement, il peut arriver que les données ne puissent être récupérées. Les plans de réversibilité doivent donc être testés et, le cas échéant, actualisés régulièrement.

Sensibiliser et former

Les actions afférentes concernent toutes les parties prenantes concernées : RH, Communication, Mar-

keting, etc. Cette sensibilisation, ces formations ont d'ores et déjà débuté, les premières actions ayant été lancées fin 2015. Pour ce faire, le CIL s'appuie sur sa propre équipe, mais aussi sur la trentaine de relais dont il dispose partout dans l'organisation.

Les participants sont sensibilisés à l'écosystème de la donnée qui repose sur le triptyque suivant : la donnée à un prix (celui du darkweb), la donnée à un coût (celui que l'entreprise supporte en cas d'incident de sécurité), la donnée a une valeur (c'est pour cela d'ailleurs qu'elle a un prix à la revente et un coût pour l'entreprise défaillante). Pour illustrer la notion d'incident de sécurité, le CIL s'appuie sur un site , qui recense les plus importantes failles depuis 2012. La valorisation du coût par donnée et par type d'incident est issue des études annuelles du Ponemon Institue Ainsi, chaque donnée compromise a représenté en 2015 un coût de l'ordre de 130 euros ; le coût (par donnée !) d'un dysfonctionnement informatique est de 120 euros environ ; une attaque malveillante se chiffre à 150 euros par donnée...

Conclusion

Le Groupe La Poste est conscient que la donnée a une valeur, qui diffère selon l'usage que l'on en fait. Dans la société numérique actuelle, la donnée a une prééminence très forte dans le fonctionnement de l'entreprise et dans les business models. Tout ce qui va affecter une donnée – si la protection de la donnée est insuffisante donc – va engendrer une perte de confiance. Or chacun sait combien cette confiance, une fois perdue, est particulièrement compliquée à rétablir.