RGPD : CAP SUR LES BONNES PRATIQUES AVEC COVATEAM

L'essor du numérique a augmenté les risques informatiques et ceux liés à la manipulation des données sensibles. C'est dans ce cadre que le RGPD a été pensé par l'UE, afin de piloter les pratiques numériques de toutes les organisations et protéger les données personnelles des individus. Comment les organisations doivent-elles s'y prendre pour l'appliquer ? Sophie Borel, Consultante RGPD et DPO externe de Covateam, nous explique comment se mettre en conformité.

Suite aux dérives d'utilisation des données par plusieurs géants du numérique, le Règlement Général de Protection des Données (RGPD) est venu instaurer des règles pour la collecte des données personnelles, leur conservation, leur stockage, leur archivage, et leur suppression à l'échelle européenne. Depuis mai 2018, il s'impose donc à toutes les organisations de l'UE qui utilisent et manipulent des données à caractère personnel.

RGPD : qui est concerné ?

Toutes les entreprises utilisant des données à caractère personnel sont concernées par le RGPD, mais, selon le type d'activité exercé et la nature des données stockées, certaines le sont plus que d'autres, C'est le cas des entreprises en B2C qui détiennent des données personnelles sur les clients, utilisées à des fins commerciales. Sont aussi concernées par ces obligations les sous-traitants, comme par exemple les prestataires de services ou de logiciels qui ont accès aux bases de données en provenance d'autres structures. Ayant indirectement accès à des données personnelles, ces derniers ont aussi tout intérêt à se mettre en conformité et à être irréprochables aux yeux du client. Sans oublier les acteurs publics, comme les collectivités, les administrations et autres organismes de la sphère publique. En effet, bien que ces organismes n'exploitent pas ces données à des fins purement commerciales, ils détiennent néanmoins des informations détaillées sur les citoyens, qu'ils sont par ailleurs dans l'obligation de préserver.

Application du RGPD : contrainte ou opportunité ?

Certaines organisations perçoivent la mise en conformité au RGPD comme une obligation, voire une contrainte additionnelle en vue d'éviter des sanctions. Dans ces structures, la mise en place s'est révélée être moins efficace que dans les entreprises qui y voient une opportunité et qui en comprennent les enjeux. Pour ces raisons-là, il est essentiel pour les entreprises d'apprécier les bénéfices que l'application du RGPD pourrait leur apporter et d'impliquer pleinement leurs équipes dans la bonne mise en place du RGPD au sein de l'organisation.

Recensement de l'état des lieux

Alors comment toutes ces organisations doivent-elles s'y prendre pour enclencher cette mise en conformité ? Et que doivent-elles savoir ? Plusieurs étapes sont à prévoir afin de répondre à ces exigences réglementaires. La première est celle du recensement.
Les organisations doivent, dans un premier temps, faire l'état des lieux en interne et d'avoir un aperçu de la façon dont chaque service utilise et conserve les données personnelles. Ont-elles mis en place des registres de traitement de leurs données personnelles ? Ces derniers recensent toutes les utilisations des données au sein de l'organisation (que ce soit au niveau des RH, du marketing ou du service commercial…).

Quel registre mettre en place ?

Cela dépend largement de la taille de l'organisation. Ainsi, les plus grandes avec de larges volumes de données stockées pourraient bénéficier de logiciels qui automatisent les registres de traitement avec différentes actions pour le rendre plus efficace. Pour les petites structures, en revanche, qui n'ont pas les moyens ou ne peuvent justifier le coût de ces logiciels, la Cnil a mis en

place un registre de traitement simplifié en format Excel. Évidemment, il convient de mentionner ici que la Cnil contrôle les registres de traitement mis en place par les organisations afin de recenser leurs usages des données à caractère personnel conservées dans leurs systèmes.

DPO : comment faire son choix ?

Sophie Borel rappelle que pour certaines organisations (les organismes publics, ceux ayant un suivi régulier des personnes, et ceux manipulant des données sensibles à large échelle), le DPO est une obligation. Ces organismes ont le choix soit d'internaliser soit de choisir une personne clé en interne, soit d'avoir recours à une personne externe à l'organisation.
Bien sûr, les collaborateurs en interne ont l'avantage d'avoir une vue transverse sur tous les services et pourraient être mieux formés pour mener leurs missions à bien. Certaines structures font par ailleurs le choix d'externaliser soit parce qu'elles n'ont pas les ressources en interne, soit pour des questions d'indépendance et d'impartialité. Enfin, toutes les organisations, si elles en voient l'intérêt, ont l'option de nommer un DPO même si elles n'en ont pas l'obligation.

Des plans d'actions adaptés

Après l'étape de recensement, les organisations doivent mettre en place un plan d'action afin de répondre aux exigences du RGPD. Elles doivent, entre autres, informer les personnes concernées de l'usage de leurs données et de leurs droits. Par ailleurs, elles doivent faire attention à ne pas conserver des données au-delà des échéances légales, et instaurer les mesures de sécurité (informatique et physique) nécessaires pour protéger ces données. En fonction de cet état des lieux et de la nature des données stockées, le plan d'action sera différent dépend des exigences réglementaires en termes de consentement écrit des personnes concernées, des durées de conservation ou de la sécurité informatique.

Covateam : analyse et accompagnement

Pour dresser au mieux le plan d'action, une analyse de risques s'impose afin de vérifier que les données utilisées n'impactent pas les personnes concernées et que toutes les mesures nécessaires ont été prises pour éviter les risques qui y sont liés. À ces fins, de par son activité de conseil, Covateam sensibilise les entreprises et leurs collaborateurs, mais aussi les collectivités, les agents, etc. afin qu'ils comprennent mieux les enjeux du RGPD et afin qu'ils puissent acquérir les outils qui peuvent répondre à leurs besoins. Covateam les accompagne ensuite dans la mise en place du plan d'action en interne et peut tenir le rôle de DPO (délégué à la protection des données) si l'organisation le souhaite.

SÉCURITÉ DES SI : SE PRÉMUNIR DE L'ERREUR HUMAINE

Si le facteur humain reste la première menace pour la cybersécurité des organisations, des solutions et des process existent pour anticiper et s'en protéger.

« Derrière 90% des failles techniques, il y a une erreur humaine », estime Thibault Carré, directeur cybersécurité du cabinet de conseils Inquest. Pour les attaquants, ces failles sont particulièrement propices au développement de leurs logiciels de rançon. Ils introduisent ainsi un code malveillant dans les systèmes d'information, empêchant la victime d'accéder à ses données sauf contre de l'argent. Ce mode d'action s'est beaucoup développé et constitue désormais la principale menace pour les SI, selon l'Agence nationale de sécurité des systèmes d'information (Anssi). Alors que 54 incidents liés à des rançongiciels lui ont été signalés en 2019, l'Agence en a dénombré 192 en 2020, soit une multiplication par quatre. Et aucun secteur d'activité ne semble épargné, des collectivités territoriales en passant par les établissements de santé ou les entreprises du secteur de l'industrie.

Des questions de coûts et de réputation

Les coûts de telles attaques sont variables, ils peuvent inclure des pertes financières et d'exploitation, mais aussi faire courir des risques aux clients et aux fournisseurs en lien avec l'organisation touchée. Les conséquences sont également lourdes en termes d'image et d'impact psychologique. Dans son dernier rapport d'activité, l'Anssi cite notamment le cas de Sopra Steria, victime du logiciel malveillant Ryuk en octobre 2020, qui a évalué ses pertes à environ 50 millions d'euros.

Les réseaux de communication, première cible

Pour éviter de tels dégâts, il convient d'identifier les différentes portes d'entrée de ces menaces. « De manière générale, ce sont tous les vecteurs de communication qu'il faut surveiller. La majorité des menaces passent par le mail, même s'il faut aussi faire attention aux canaux plus récents comme les plates-formes collaboratives sur lesquelles on échange beaucoup de messages entre collègues », détaille Laura Peytavin, ingénieure consultante avant-vente en systèmes de cybersécurité chez l'éditeur américain Proofpoint. La raison est assez simple, il suffit de se mettre à la place des pirates selon l'experte : « Le mail est le vecteur de menaces qui ne coûte presque rien à mettre à en œuvre. La cybermalveillance est aussi une question d'économie. Les instigateurs ciblent les collaborateurs pour faire à leur place le premier geste fatal du clic sur un lien ou une pièce jointe malicieux, bénéficiant de leur adresse électronique présente dans toutes les traces électroniques que nous laissons un peu partout et qui sont volées. »

Des systèmes et logiciels qui ne sont pas à jour

ssi explique aussi la recrudescence des attaques par un manque de mise à jour des systèmes et des applications, une politique de gestion des mots de passe insuffisante ou encore un laxisme dans les autorisations de droits d'accès externes au SI. Le développement du télétravail au cours de la pandémie n'a pas aidé à contrer ces défaillances. « Corréler la hausse des incidents avec la crise sanitaire n'est pas si évident. Il y avait déjà une activité de cyberattaques en forte augmentation depuis quelques années, mais il est vrai que le contexte a favorisé dans une certaine mesure la multiplication des portes d'entrée pour les pirates », note Thibault Carré.

Se protéger et anticiper

Face à ce constat, des solutions existent, notamment techniques, comme des logiciels à base d'intelligence artificielle et de machine learning qui apprennent à identifier les menaces et à les bloquer. « L'IA n'est pas une boîte magique, mais un outil très puissant. Nous l'utilisons car les attaquants ont déjà ces technologies. Quand ceux-ci s'attachent à cartographier les vulnérabilités des cibles, le facteur humain, nous utilisons en retour les outils de big data pour suivre à la trace le profil des moyens et des stratégies de leurre qu'ils utilisent en temps réel », révèle Laura Peytavin.

Sensibiliser les collaborateurs aux risques cyber

A cet outillage s'ajoutent des formations spécifiques qui ne sont pas assez systématisées selon Thibault Carré : « L'idéal serait d'instaurer des cessions de sensibilisation au sein des entreprises comme c'est le cas avec les alertes incendie. Tout le monde saurait alors réagir face à une demande étrange. » Les outils les plus efficaces selon Proofpoint sont ceux qui allient une forte capacité de protection et la participation des collaborateurs. Ces derniers peuvent par exemple être amenés à signaler et obtenir en un clic l'analyse d'un mail qui leur semble suspect. La machine apprend ainsi au fur et à mesure à identifier davantage de menaces. Une boucle vertueuse de protection se met alors en place entre l'humain et l'intelligence artificielle

S'assurer pour limiter les pertes financières

Enfin, en plus de la prévention et de la formation à la gestion de crise, il est aussi préférable de recourir à une cyberassurance pour se protéger. « En aval, l'assurance permet de financer la gestion de crise avec des experts en cyber assistance, les frais de notification en cas de perte des données, ainsi que tous les dommages financiers liés directement ou indirectement à l'attaque », rappelle l'Association pour le management des risques et des assurances de l'entreprise (Amrae) dans son étude "Lucy" publiée en mai 2021. Les auteurs insistent sur le fait que si 87 % des grandes entreprises disposent d'un contrat d'assurance cyber, leur niveau de couverture semble très inférieur à leur exposition au risque. Cependant, le plus inquiétant reste le taux de couverture des ETI qui s'élève à seulement 8 %. Cette situation est un « frein au développement du marché l'assurance cyber », juge l'Amrae, « les assureurs peinent à trouver un modèle économique viable ».

Un ROI à calculer

Les assureurs sont d'autant plus fragilisés que le montant des indemnisations versés suite à un sinistre a été multiplié par trois entre 2019 et 2020, passant de 73 millions à 217 millions d'euros. A l'avenir, les cyberassurances risquent de coûter plus cher, alors même que le risque, et donc la nécessité d'y souscrire, vont devenir plus pressants pour les organisations. Toutefois le grand débat des mois à venir reste le versement ou non de la rançon en cas d'attaque. Certaines assurances préfèrent céder, estimant que cela coûte moins cher que de couvrir les conséquences de la perte totale des données volées. Mais cette méthode ne fait qu'encourager l'activité des hackers pour l'Anssi. Tous ces acteurs réclament actuellement que les législateurs tranchent la question.

La confiance Numérique par Covateam