

Des « logiciels RGPD » pour se mettre en conformité avec le règlement européen

Description

Depuis l'entrée en vigueur du règlement européen sur la protection des données personnelles (RGPD), le 25 mai 2018, une offre logicielle se développe, celle de la Cnil notamment, qui permet à n'importe quelle organisation traitant des données sensibles de se mettre en conformité avec le règlement.

L'esprit du règlement européen sur la protection des données personnelles repose sur une responsabilisation accrue et un renforcement des exigences à l'égard des auteurs de traitements de données personnelles, afin notamment qu'ils assurent « *une protection optimale des données à chaque instant et soient en mesure de la démontrer en documentant leur conformité* » ([voir La rem n°42-43, p.21](#)). Autrement dit, les organisations n'ont plus à effectuer une déclaration de détention de données personnelles *a priori*, comme c'était le cas avec la loi dite Informatique et libertés du 6 janvier 1978, mais elles doivent être en mesure de prouver à tout moment, par l'intermédiaire de leur délégué à la protection des données (DPO pour Data Protection Officer), que les traitements de données opérées sont bien conformes à la législation en vigueur.

De nombreux éditeurs de logiciels proposent, pour certains depuis 2017, des solutions informatiques permettant d'automatiser leur mise en conformité avec la législation imposée par le règlement européen, parmi lesquels Data Flow Map, Smart Global Privacy, Compliance Booster, Captain DPO, Data Legal Drive, RGPD Manager, GDPR Compliance Solution, myDPO, Mission RGPD, EKIALIS Explore, DPMS, Blockproof, Central Consent Manager, GDPR Drop, Power GDPR, Aseptio, DATAE, DPO.run, Actecil Privacy Manager ou encore Adequacy. Face à cette offre pléthorique de logiciels propriétaires, le Laboratoire d'innovation numérique de la Cnil (LINC) développe, depuis 2017, le logiciel PIA (Privacy Impact Assessment), distribué librement et dont l'objet est de faciliter la conduite et la formalisation d'analyses d'impact relatives à la protection des données (AIPD), telles que prévues par le RGPD.

Cette fonctionnalité d'analyse d'impact se retrouve à la fois dans l'offre logicielle libre et propriétaire. L'article 35 du RGPD prévoit la conduite d'une telle analyse, « *lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées* ». La notion de risque élevé s'apprécie au regard d'une liste prévue par le règlement européen. Elle concerne notamment le traitement des données génétiques des personnes dites vulnérables (patients, employés, enfants, etc.) et des données de santé recueillies par les établissements de santé ou les établissements médico-sociaux pour la prise en charge de ces personnes ; le traitement établissant des profils de personnes physiques à des fins de gestion des ressources humaines ; le traitement ayant pour finalité de surveiller de manière constante l'activité des employés concernés ; le traitement impliquant le profilage des personnes pouvant aboutir à l'exclusion du bénéfice d'un contrat ou à sa suspension, voire à sa rupture ; le traitement de profilage faisant appel à des données qui proviennent de sources externes ou encore le

traitement de données de localisation à large échelle.

Dès lors qu'une organisation recueille et analyse ce type de données, elle doit obligatoirement prévoir une analyse d'impact relative à la protection des données (AIPD) qui se décompose en trois parties : « (1) Une description détaillée du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels. (2) L'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes, etc.) non négociables, qui sont fixés par la loi et doivent être respectés, quels que soient les risques. (3) L'étude, de nature plus technique, des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données ».

Le logiciel PIA de la Cnil, dont la première version disponible en téléchargement date de novembre 2017, a pour objectif de « faciliter la réalisation d'analyses d'impact sur la protection des données prévues par le RGPD ». Le logiciel peut être lancé sur un poste de travail ou être déployé sur les serveurs d'une organisation, afin d'être intégré dans les outils existant en interne. Selon Estelle Hary, designer à la Cnil, le logiciel s'articule autour de trois axes et consiste à suivre la méthodologie prévue par le règlement européen. Tout d'abord, la description et le contexte du traitement de données permettent de se poser les bonnes questions : « *Quel est mon traitement et ses enjeux principaux ? Quelles sont les données traitées et comment le sont-elles ? Quelles sont les réglementations auxquelles mon traitement est soumis ?* ». Le deuxième axe concerne l'étude juridique du traitement de données personnelles et sa mise en œuvre : « *Respecte-t-il les principes de proportionnalité et de nécessité ? Par exemple, sa finalité est-elle clairement définie ? Est-ce que les personnes concernées par le traitement sont correctement informées à propos de mon traitement ? Comment peuvent-elles faire valoir leurs droits ?* ». Enfin, l'évaluation des risques permet de prendre en compte l'analyse préalablement effectuée et d'y répondre par des mesures techniques, comme l'anonymisation ou le chiffrement, et des mesures organisationnelles, comme celles liées à la gestion du personnel. Le logiciel permet ensuite de visualiser, à travers un tableau de bord, les risques liés au traitement des données personnelles et de prendre les mesures nécessaires pour les limiter.

Le logiciel PIA a d'abord été lancé en français et en anglais, puis traduit grâce à une communauté de bénévoles en 18 langues. Référencé sur le site de l'OCDE parmi les initiatives exemplaires en matière d'innovation publique, il a également été récompensé en 2018 par deux « Global Privacy and Data Protection Awards », lors de l'International Conference of Data Protection and Privacy Commissioners (ICDPPC) réunissant, chaque année depuis 1979, les autorités administratives indépendantes équivalentes à la Cnil à travers le monde.

En décembre 2018, le logiciel a été téléchargé 130 000 fois. Puisqu'il est open source, quiconque peut y contribuer ou développer une version alternative. En octobre 2019, le logiciel a fait l'objet de 193 *forks*, ramifications informatiques qui gardent à la fois les fonctions existantes et en rajoutent de nouvelles.

C'est notamment le cas d'une version alternative développée par Libre Informatique sous le nom de PIA

Lab, comptant une quinzaine de clients parmi lesquels une institution médico-sociale qui regroupe 150 établissements en France et qui manipule des données sensibles liées à des situations de handicap et à des personnes âgées. Libre Informatique, société coopérative et participative (SCOP), membre de Coopaname, mutuelle de travail associée créée en 2004, a souhaité développer une version alternative à celle de la Cnil pour répondre aux besoins de certains clients liés à l'authentification des utilisateurs du logiciel afin de travailler de manière collaborative, et pour les accompagner sur la prise en main du logiciel. En effet, selon Amélie Caro, consultante RGPD pour PiaLab, « *entre l'offre de la Cnil, dont certaines fonctionnalités n'étaient pas encore assez abouties et l'offre des logiciels propriétaires, dont les fonctionnalités sont au contraire bien trop nombreuses, certains clients se sentent un peu perdus* ».

Les fonctionnalités proposées par les logiciels propriétaires recoupent celles proposées par le logiciel PIA : cartographier les traitements de données personnelles, identifier les données sensibles, gérer les droits et demandes. Ces logiciels permettent ainsi de tenir des registres des risques et des mesures, d'enregistrer l'agrément des parties prenantes, de faire remonter des déclarations d'incidents, d'être alerté en cas d'anomalies : un travail collaboratif où sont précisément définis les utilisateurs et le rôle de chacun, le tout étant supervisé par le délégué à la protection des données personnelles. Certains logiciels sont préconfigurés par secteurs d'activité ou par métiers afin de mieux guider le DPO dans la cartographie des traitements. Ces logiciels intègrent parfois des modules de formation permettant d'accompagner les parties impliquées dans la protection des données. Proposés à partir d'une centaine d'euros par mois, les tarifs évoluent suivant la taille de la structure au sein de laquelle le logiciel est déployé. Tous ont pour principal argument de faire gagner un temps précieux aux entreprises en automatisant en grande partie des règles de conformité à la réglementation en vigueur.

Sources :

- « [outil] Le PIA pas à pas », Estelle Hary, Laboratoire d'innovations numériques de la Cnil (LINC), linc.cnil.fr, 22 novembre 2017.
- « RGPD – La Cnil propose un logiciel libre PIA pour soigner sa conformité », Christophe Auffray, zdnet.fr, 19 janvier 2018.
- « RGPD et logiciels libres pour accompagner les mises en conformité », Baptiste Simon, linuxfr.org, 1^{er} mai 2018.
- « Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD) », cnil.fr, 6 novembre 2018.
- « Analyse d'impact : la version 2.0 de l'outil PIA est disponible », cnil.fr, 6 décembre 2018.
- « Quels outils logiciels pour la mise en conformité au RGPD », Xavier Biseul, zdnet.fr, 23 juillet 2019.
- « Outil PIA : téléchargez et installez le logiciel de la Cnil », cnil.fr, 5 août 2019.
- « Smart Global Privacy, un outil de détection automatisée des non-conformités au RGPD », Alice Vitard, usine-digitale.fr, 10 septembre 2019.

Categorie

1. Techniques

date créée

21 janvier 2020

Auteur

jacquesandrefines