Des Â«Â logiciels RGPDÂ Â» pour se mettre en conformitÃ© avec le rÃ¨glement europÃ©en

Description

Depuis lâ€™entrÃ©e en vigueur du rÃ¨glement europÃ©en sur la protection des donnÃ©es personnelles (RGPD), le 25 mai 2018, une offre logicielle se dÃ©veloppe, celle de la Cnil notamment, qui permet Ã nâ€™importe quelle organisation traitant des donnÃ©es sensibles de se mettre en conformitÃ© avec le rÃ¨glement.

Lâ€™esprit du rÃ¨glement europÃ©en sur la protection des donnÃ©es personnelles repose sur une responsabilisation accrue et un renforcement des exigences Ã lâ€™Ã©gard des auteurs de traitements de donnÃ©es personnelles, afin notamment quâ€™ils assurentÂ *Â«Â une protection optimale des donnÃ©es Ã chaque instant et soient en mesure de la dÃ©montrer en documentant leur conformitÃ©Â Â»*Â (voirÂ *La rem*Â nÂ°42-43, p.21). Autrement dit, les organisations nâ€™ont plus Ã effectuer une dÃ©claration de dÃ©tention de donnÃ©es personnellesÂ *a priori*, comme câ€™Ã©tait le cas avec la loi dite Informatique et libertÃ©s du 6 janvier 1978, maisÂ ellesÂ doivent Ãªtre en mesure de prouver Ã tout moment, par lâ€™intermÃ©diaire de leur dÃ©lÃ©guÃ© Ã la protection des donnÃ©es (DPO pour Data Protection Officer), que les traitements de donnÃ©es opÃ©rÃ©es sont bien conformes Ã la lÃ©gislation en vigueur.

De nombreux Ã©diteurs de logiciels proposent, pour certains depuis 2017, des solutions informatiques permettant dâ€™automatiser leur mise en conformitÃ© avec la lÃ©gislation imposÃ©e par le rÃ¨glement europÃ©en, 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, Axeptio, DATAE, DPO.run, Actecil Privacy Manager ou encore Adequacy. Face Ã cette offre plÃ©thorique de logiciels propriÃ©taires, le Laboratoire dâ€™innovation numÃ©rique de la Cnil (LINC) dÃ©veloppe, depuis 2017, le logiciel PIA (Privacy Impact Assessment), distribuÃ© librement et dont lâ€™objet est de faciliter la conduite et la formalisation dâ€™analyses dâ€™impact relatives Ã la protection des donnÃ©es (AIPD), telles que prÃ©vues par le RGPD.

Cette fonctionnalitÃ© dâ€™analyse dâ€™impact se retrouve Ã la fois dans lâ€™offre logicielle libre et propriÃ©taire. Lâ€™article 35 du RGPD prÃ©voit la conduite dâ€™une telle analyse,Â *Â«Â lorsquâ€™un traitement de donnÃ©es personnelles est susceptible dâ€™engendrer un risque Ã©levÃ© pour les droits etÂ libertÃ©s des personnes concernÃ©esÂ Â»*.Â La notion de risque Ã©levÃ© sâ€™apprÃ©cie au regard dâ€™une liste prÃ©vue par le rÃ¨glement europÃ©en.Â Elle concerne notamment le traitement des donnÃ©es gÃ©nÃ©tiques des personnes dites vulnÃ©rables (patients, employÃ©s, enfants, etc.) et des

donnÃ©es de santÃ© recueillies par les Ã©tablissements de santÃ© ou les Ã©tablissements mÃ©dico-sociaux pour la prise en charge de ces personnesÂ ; le traitement Ã©tablissant des profils de personnes physiques Ã des fins de gestion des ressources humainesÂ ; le traitement ayant pour finalitÃ© de surveiller de maniÃ¨re constante lâ€™activitÃ© des employÃ©s concernÃ©sÂ ; le traitement impliquant le profilage des personnes pouvant aboutir Ã lâ€™exclusion du bÃ©nÃ©fice dâ€™un contrat ou Ã sa suspension, voire Ã sa ruptureÂ ; le traitement de profilage faisant appel Ã des donnÃ©es qui proviennent de sources externes ou encore le traitement de donnÃ©es de localisation Ã large Ã©chelle.

DÃ¨s lors quâ€™une organisation recueille et analyse ce type de donnÃ©es, elle doit obligatoirement prÃ©voir une analyse dâ€™impact relative Ã la protection des donnÃ©es (AIPD) qui se dÃ©compose en trois partiesÂ :Â *Â«Â (1) Une description dÃ©taillÃ©e du traitement mis en Å“uvre, comprenant tant les aspects techniques quâ€™opÃ©rationnels. (2) Lâ€™Ã©valuation, de nature plus juridique, de la nÃ©cessitÃ© et deÂ la proportionnalitÃ© concernant les principes et droits fondamentaux (finalitÃ©, donnÃ©es et durÃ©es de conservation, information et droits des personnes, etc.) non nÃ©gociables, qui sont fixÃ©s par la loi et doivent Ãªtre respectÃ©s, quels que soient les risques. (3) Lâ€™Ã©tude, de nature plus technique, des risques sur la sÃ©curitÃ© des donnÃ©es (confidentialitÃ©, intÃ©gritÃ© et disponibilitÃ©) ainsi que leurs impacts potentiels sur la vie privÃ©e, qui permet de dÃ©terminer les mesures techniques et organisationnelles nÃ©cessaires pour protÃ©ger les donnÃ©esÂ Â»*.

Le logiciel PIA de la Cnil, dont la premiÃ¨re version disponible en tÃ©lÃ©chargement date de novembre 2017, a pour objectif deÂ *Â«Â faciliter la rÃ©alisation dâ€™analyses dâ€™impact sur la protection des donnÃ©es prÃ©vues par le RGPDÂ Â»*.Â Le logiciel peut Ãªtre lancÃ© sur un poste de travail ou Ãªtre dÃ©ployÃ© sur les serveurs dâ€™une organisation, afin dâ€™Ãªtre intÃ©grÃ© dans les outils existant en interne. Selon Estelle Hary, designer Ã la Cnil, le logiciel sâ€™articule autour de trois axes et consiste Ã suivre la mÃ©thodologie prÃ©vue par le rÃ¨glement europÃ©en. Tout dâ€™abord, la description et le contexte du traitement de donnÃ©es permettent de se poser les bonnes questionsÂ :Â *Â«Â Quel est mon traitement et ses enjeux principauxÂ ? Quelles sont les donnÃ©es traitÃ©es et comment le sont-ellesÂ ? Quelles sont les rÃ©glementations auxquelles mon traitement est soumisÂ ?Â Â»*. Le deuxiÃ¨me axe concerne lâ€™Ã©tude juridique du traitement de donnÃ©es personnelles et sa mise en Å“uvreÂ :Â *Â«Â Respecte-t-il les principes de proportionnalitÃ© et de nÃ©cessitÃ©Â ? Par exemple, sa finalitÃ© est-elle clairement dÃ©finieÂ ?Â Est-ceÂ que les personnes concernÃ©es par le traitement sont correctement informÃ©es Ã propos de mon traitementÂ ? Comment peuvent-elles faire valoir leurs droitsÂ ?Â Â»*. Enfin, lâ€™Ã©valuation des risques permet de prendre en compte lâ€™analyse prÃ©alablement effectuÃ©e et dâ€™y rÃ©pondre par des mesures techniques, comme lâ€™anonymisation ou le chiffrement, et des mesures organisationnelles, comme celles liÃ©es Ã la gestion du personnel. Le logiciel permet ensuite de visualiser, Ã travers un tableau de bord, les risques liÃ©s au traitement des donnÃ©es personnelles et de prendre les mesures nÃ©cessaires pour les limiter.

Le logiciel PIA a dâ€™abord Ã©tÃ© lancÃ© en franÃ§ais et en anglais, puis traduit grÃ¢ce Ã une communautÃ© de bÃ©nÃ©voles en 18 langues. RÃ©fÃ©rencÃ© sur le site de lâ€™OCDE parmi les initiatives exemplaires en matiÃ¨re dâ€™innovation publique,Â il a Ã©galement Ã©tÃ© rÃ©compensÃ©

en 2018 par deuxÂ Â«Â Global Privacy and Data Protection AwardsÂ Â», lors de lâ€™International Conference of Data Protection and Privacy Commissioners (ICDPPC)Â rÃ©unissant, chaque annÃ©e depuis 1979, les autoritÃ©s administratives indÃ©pendantes Ã©quivalentes Ã la Cnil Ã travers le monde.

En dÃ©cembre 2018, le logiciel a Ã©tÃ© tÃ©lÃ©chargÃ©Â 130 000Â fois. Puisquâ€™il est open source, quiconque peut y contribuer ou dÃ©velopper une version alternative. En octobre 2019, le logiciel a fait lâ€™objet de 193Â *forks*, ramifications informatiques qui gardent Ã la fois les fonctions existantes et en rajoutent de nouvelles.

Câ€™est notamment le cas dâ€™une version alternative dÃ©veloppÃ©e par Libre Informatique sous le nom de PIA Lab, comptant une quinzaine de clients parmi lesquels une institution mÃ©dico-sociale qui regroupe 150 Ã©tablissements en France et qui manipule des donnÃ©es sensibles liÃ©es Ã des situations de handicap et Ã des personnes Ã¢gÃ©es. Libre Informatique, sociÃ©tÃ© coopÃ©rative et participative (SCOP), membre de Coopaname, mutuelle de travail associÃ©e crÃ©Ã©e en 2004, a souhaitÃ© dÃ©velopper une version alternative Ã celle de la Cnil pour rÃ©pondre aux besoins de certains clients liÃ©s Ã lâ€™authentification des utilisateurs du logiciel afin de travailler de maniÃ¨re collaborative, et pour les accompagner sur la prise en main du logiciel. En effet, selon AmÃ©lie Caro, consultante RGPD pour PiaLab,Â *Â«Â entre lâ€™offre de la Cnil, dont certaines fonctionnalitÃ©s nâ€™Ã©taient pas encore assez abouties et lâ€™offre des logiciels propriÃ©taires, dont les fonctionnalitÃ©s sont au contraire bien trop nombreuses, certains clients se sentent un peu perdusÂ Â»*.

Les fonctionnalitÃ©s proposÃ©es par les logiciels propriÃ©taires recoupent celles proposÃ©es par le logiciel PIAÂ : cartographier les traitements de donnÃ©es personnelles, identifier les donnÃ©es sensibles, gÃ©rer les droits et demandes. Ces logiciels permettent ainsi de tenir des registres des risques et des mesures, dâ€™enregistrer lâ€™agrÃ©ment des parties prenantes, de faire remonter des dÃ©clarations dâ€™incidents, dâ€™Ãªtre alertÃ© en cas dâ€™anomaliesÂ : un travail collaboratif oÃ¹ sont prÃ©cisÃ©ment dÃ©finis les utilisateurs et le rÃ´le de chacun, le tout Ã©tant supervisÃ© par le dÃ©lÃ©guÃ© Ã la protection des donnÃ©es personnelles. Certains logiciels sont prÃ©configurÃ©s par secteurs dâ€™activitÃ© ou par mÃ©tiers afin de mieux guider le DPO dans la cartographie des traitements. Ces logiciels intÃ¨grent parfois des modules de formation permettant dâ€™accompagner les parties impliquÃ©es dans la protection des donnÃ©es. ProposÃ©s Ã partir dâ€™une centaine dâ€™euros par mois, les tarifs Ã©voluent suivant la taille de la structure au sein de laquelle le logiciel est dÃ©ployÃ©.Â Tous ont pour principal argument de faire gagner un temps prÃ©cieux aux entreprises en automatisant en grande partie des rÃ¨gles de conformitÃ© Ã la rÃ©glementationÂ en vigueur.

Sources :

- Â« [outil] Le PIA pas Ã pas Â», Estelle Hary, Laboratoire dâ€™innovations numÃ©riques de la Cnil (LINC), linc.cnil.fr, 22 novembre 2017.
- Â« RGPD â€“ La Cnil propose un logiciel libre PIA pour soigner sa conformitÃ© Â», Christophe Auffray, zdnet.fr, 19 janvier 2018.
- Â« RGPD et logiciels libres pour accompagner les mises en conformitÃ© Â», Baptiste Simon,

linuxfr.org, 1er mai 2018.
- Â« Ce qu'il faut savoir sur lâ€™analyse dâ€™impact relative Ã la protection des donnÃ©es (AIPD) Â», cnil.fr, 6 novembre 2018.
- Â« Analyse dâ€™impact : la version 2.0 de lâ€™outil PIA est disponible Â», cnil.fr, 6 dÃ©cembre 2018.
- Â« Quels outils logiciels pour la mise en conformitÃ© au RGPD Â», Xavier Biseul, zdnet.fr, 23 juillet 2019.
- Â« Outil PIA : tÃ©lÃ©chargez et installez le logiciel de la Cnil Â», cnil.fr, 5 aoÃ»t 2019.
- Â« Smart Global Privacy, un outil de dÃ©tection automatisÃ©e des non-conformitÃ©s au RGPD Â», Alice Vitard, usine-digitale.fr, 10 septembre 2019.

Categorie

1. Techniques

date crÃ©Ã©e
21 janvier 2020
Auteur
jacquesandrefines