_swissprivacy.law

Le registre des activités de traitement, un outil de pilotage essentiel

Elodie Pierloot, le 17 avril 2024

Pour beaucoup, le registre des activités de traitement n'est autre qu'un inventaire à la Prévert long et fastidieux, que l'on dépoussière de temps à autre, au cas où il viendrait à l'idée d'un régulateur ou d'une autorité de contrôle de venir fouiner. Et pourtant, le registre des activités de traitement constitue une mine d'or s'il est bâti et maintenu correctement et peut même s'avérer être un outil de pilotage précieux, non seulement pour le DPO, mais pour l'organisation tout entière. Lumière donc sur ce dispositif mal aimé de la protection des données.

I. Introduction

J'ai débuté ma carrière dans le secteur bancaire en 2007. À cette époque, Bâle II était sur toutes les lèvres et la gestion des risques commençait à véritablement se renforcer dans les institutions bancaires. Pour mémoire, cette réglementation internationale du secteur bancaire a été publiée par le comité de Bâle en 2004, traduit dans une directive européenne en 2006 et entrée en vigueur à partir de 2007. Il a depuis lors été remplacé par Bâle III, en vigueur depuis 2023. Ce dispositif prudentiel visait à mieux appréhender les risques bancaires en définissant des exigences minimums en capital (pilier I), un cadre de supervision réglementaire (pilier II) et une obligation de transparence (pilier III). Ces directives étaient en majorité destinées à gérer le risque de crédit et de contrepartie, mais il introduisait également la notion de risques opérationnels, c'est-à-dire, pour faire simple, les risques non bancaires. Parmi les exigences du pilier I, il était attendu des banques qu'elles établissent une cartographie des risques opérationnels auxquels elles étaient exposées. De vastes chantiers ont été lancés dans toutes les institutions financières pour inventorier les risques, les documenter et les évaluer. Ces cartographies longues et indigestes au départ sont devenues, pour la plupart et en une dizaine d'années, de véritables outils de pilotage des risques. Il aura fallu du temps et de sérieux efforts pour les enrichir, les interconnecter, les rationaliser et mettre en place une gouvernance robuste afin qu'elles deviennent des outils de gestion du risque indispensables à toute institution financière.

Lorsque j'ai rejoint l'univers de la protection des données en 2017, alors que le RGPD commençait à faire trembler bon nombre d'organisations internationales en Suisse, j'ai pu

observer de nombreuses similitudes quant à la manière d'appréhender la constitution du *Record of Processing Activities* (RoPA), ou registre des activités de traitement en bon français. Dans cette contribution, je dévoile quelques-uns enseignements que j'ai tiré de mon expérience dans la gestion des risques opérationnels, et je fournis quelques pistes sur la manière de les appliquer pour rapidement gagner en maturité et faire du registre des activités de traitement un outil de pilotage essentiel.

II. Qu'est-ce au juste qu'un registre des activités de traitement ?

a) Ce que dit la loi

Selon l'art. 12 LPD, les responsables du traitement et les sous-traitants tiennent chacun un registre de leurs activités de traitement. Cet article est largement inspiré, si ce n'est quasi copié-collé, de l'art. 30 RGPD. Les organes fédéraux doivent en outre déclarer ce registre au PFPDT, contrairement aux entreprises privées qui n'y sont pas tenues. Les entreprises privées de moins de 250 employés sont exemptées à la fois par l'art. 12 al. 5 LPD et l'art. 30 al. 5 RGPD, si tant est que les activités de traitement ne présentent pas de risque élevé d'atteinte aux personnes. Les lois cantonales en matière de protection des données imposent elles aussi généralement la tenue et la publication des registres d'activités de traitements par les entités cantonales ou communales. C'est par exemple le cas dans les cantons de Fribourg et du Valais.

Les informations à collecter listées à l'art. 12 al. 2 LPD se rapportent à la nature, à la finalité et aux personnes responsables de l'activité de traitement des données, à la nature des données personnelles et ceux à qui elles se rapportent, à leurs destinataires et le cas échéant, au pays récipiendaire, à la durée de conservation et enfin aux mesures de sécurité. De nombreux modèles et des outils répondant aux critères du RGPD sont disponibles depuis quelques années, certains mis à disposition par les autorités de contrôle elles-mêmes comme la CNIL en France ou l'ICO au Royaume-Uni, et permettent d'établir son registre sans trop se poser de question.

b) Ce qu'il en est

Bon nombre d'organisations se sont lancées dans des programmes de recensement des activités de traitement des données, certaines en déroulant des questionnaires à travers toute l'organisation, d'autres en réutilisant des inventaires de processus préexistants, d'autres enfin en partant d'inventaires informatiques et/ou de résultats d'outils de discovery.

Quelle que soit la démarche adoptée, ces premières versions du registre auront eu le mérite de rassurer la direction sur la conformité à la loi et de sensibiliser un certain nombre de collaborateurs sur la problématique de la protection des données. Ces premières versions peuvent cependant présenter encore aujourd'hui de nombreuses faiblesses qui en font pour bon nombre d'organisations une contrainte plutôt qu'un atout, à l'instar des premières cartographies de risques opérationnels :

- En motivant leur élaboration uniquement par la volonté de satisfaire aux besoins de conformité avec très peu si ce n'est aucun bénéfice perceptible, ces démarches ont pu générer un désengagement voir une méfiance à la fois de la part de la direction et des collaborateurs.
- En adoptant une approche dite « *bottom-up* », c'est-à-dire en interrogeant de nombreux collaborateurs ou en épluchant des inventaires IT très détaillés, ces démarches ont pu engendrer un catalogue long, trop détaillé et incohérent.
- En faisant appel à des consultants externes, en réutilisant des catalogues préexistants et/ou en utilisant des outils de discovery, ces démarches ont pu entraîner un manque d'implication et une déresponsabilisation des collaborateurs en interne.
- En réclamant beaucoup de temps et d'efforts, ces démarches ont pu tout simplement fatiguer et démotiver les parties prenantes, laissant ces registres « dans leur jus » et abandonnés de tous.

Toutes les organisations n'ont pas nécessairement été confrontées à ces difficultés. Cela dit, quel que soit son état d'avancement, il est peut-être temps de prendre du recul et de s'interroger sur l'utilité et l'efficacité de son registre des activités de traitement afin d'en optimiser le ratio coûts/bénéfices.

III. Quels bénéfices en tirer ?

a) Connaître ses données

Si ces articles sont présents dans la LPD et dans le RGPD, c'est pour une bonne raison : le registre des activités de traitement constitue la meilleure des preuves que l'organisation sait ce qu'elle fait de toutes les données personnelles qu'elle traite. Plus le registre est de qualité et à jour, plus il est vraisemblable que l'organisation sait, voire maîtrise ce qui s'y passe. C'est la raison pour laquelle le registre des activités de traitement est sans conteste le premier justificatif demandé par l'autorité de protection des données en cas d'enquête. Cela dit, d'autres parties prenantes en interne comme les fonctions d'audit, de conformité ou de gestion des risques peuvent aussi avoir un intérêt à consulter ce registre. Il peut leur

permettre d'enrichir leurs sources d'information pour mener à bien leurs évaluations et investigations, d'appréhender certaines problématiques sous un angle différent ou d'affiner leurs identifications et évaluations des risques.

b) Instaurer la confiance

La loi fédérale sur le principe de la transparence dans l'administration fédérale a pour but, en complément de la LPD, de réinstaurer la confiance dans les institutions publiques. Selon l'art. 1 LTrans, elle a pour objet de promouvoir la transparence quant à la mission, l'organisation et l'activité de l'administration. En allant au-devant de déclarant un registre exhaustif et de qualité, non seulement auprès du PFPDT ou du préposé cantonal, mais également auprès de ses concitoyens, l'administration peut envoyer un signal fort quant à la légitimité et le sérieux avec lequel elle traite des données personnelles. Dans le secteur privé, les sous-traitants ont également tout intérêt à partager un registre de qualité avec leurs clients pour les assurer de la conformité du traitement des données qui leur sont confiées. Partager intégralement ce type de documents en l'état n'est pas toujours possible, mais en publier une partie, un résumé ou en expliciter les fondements peut apporter plus de transparence et de crédibilité auprès des clients, partenaires, employés ou toute autre partie prenante à l'entreprise.

c) Cibler les remédiations

Un bon registre des activités peut être un outil très puissant lorsqu'il s'agit d'évaluer l'ampleur, la teneur et de tracer les contours de futurs programmes de remédiation. Chaque année, de nouvelles lois relatives à la protection des données sont adoptées de par le monde, comme le *Digital Personal Data Protection Act* en Inde en 2023. Chaque année, de nouveaux arrêts enrichissent la jurisprudence, voire bouleversent des pratiques jusqu'alors acceptables. Chaque année enfin, de nouvelles technologies telles que l'IA générative, de nouvelles pratiques telles que l'abandon des cookies tiers ou même des réorganisations purement internes peuvent amener à lancer des programmes de petite ou de grande ampleur. Estimer l'impact sur le traitement des données, anticiper les problèmes et les résoudre proactivement sera nettement plus aisé si le registre des activités de traitement est complet, à jour et bien structuré.

d) Rationaliser les processus

À peu près toutes les exigences liées à la protection des données peuvent être reliées de près ou de loin au registre des activités de traitement et optimisées. Par exemple :

- Ce qui est inscrit dans la politique de protection des données peut être un résumé du registre des activités de traitement.
- La source d'information pour répondre à une demande de droit d'accès peut être plus facilement identifiée en consultant le registre des activités de traitement.
- Avant d'entamer une étude d'impact sur un processus préexistant, le registre des activités de traitement permet de comprendre le contexte de l'activité dans son ensemble, d'avoir une évaluation du risque préexistant et de n'évaluer que le risque incrémenté ou consolidé.

Et inversement, opérer ces contrôles en lien étroit avec le registre des activités permettra de l'enrichir, de le challenger et de l'améliorer.

Au-delà même des processus purement liés à la protection des données, le registre des activités peut être un excellent point de départ pour réfléchir à l'efficacité des processus internes, à l'expérience client ou au positionnement de la marque ou des valeurs de l'organisation. À titre d'exemple, le consentement utilisé comme base juridique dans plusieurs processus différents, est-il toujours collecté et géré effectivement et efficacement ? L'expérience client de collecte du consentement est-elle cohérente et fluide ?

e) Gérer les risques

Après y avoir ajouté une composante risque, le registre des activités de traitement peut rapidement devenir un outil de gestion des risques très utile, à la fois pour soutenir un dispositif de surveillance opérationnel des contrôles, mais également pour apporter une vue d'ensemble stratégique et faciliter la prise de décision. En classifiant, évaluant et/ou en hiérarchisant les activités et les flux de données, il devient possible de répondre à un certain nombre de questions, par exemple :

- En surveillant des indicateurs clés par rapport à des seuils d'alerte : Le volume de transferts à l'étranger est-il acceptable ? Dans combien de pays différents transmettons-nous des données et, après pondération du risque par pays, quelle est notre exposition ? La quantité de données sensibles récoltées est-elle en adéquation avec l'activité de l'organisation ? Quelle est l'exposition au risque de manière consolidée et où se situe-t-elle par rapport au seuil de tolérance ?
- En identifiant les activités les plus exposées à un risque : Comment cibler ses actions de communication et de formation ? Quelles équipes doivent être davantage surveillées par des dispositifs de sécurité ?
- En établissant des scénarios de risque pour évaluer l'impact d'un changement interne

ou externe et anticiper ses effets : Que se passerait-il si la loi de protection des données chinoise (ndlr la PIPL qui restreint considérablement les possibilités de transferts hors de Chine) s'étendait aux provinces autonomes, et notamment Hong-kong ? Que se passerait-il si un logiciel externe était jugé non conforme, comme suite aux 101 plaintes déposées en 2020 par NOYB contre des utilisateurs de Google Analytics et Facebook Connect ?

Toutes ces questions et bien d'autres encore trouveront leurs réponses dans le registre des activités de traitement en y appliquant une vue centrée sur le risque.

IV. Comment l'élaborer de manière efficace ?

Construire et maintenir un registre des activités de traitement a un coût, qui ne fera qu'augmenter à mesure qu'il deviendra plus sophistiqué et profitable à l'organisation. En contenir l'augmentation permet de sécuriser et d'optimiser les ressources nécessaires et de le rendre viable sur long terme.

a) Faire simple et proportionné

Tout d'abord, réduire la granularité des activités listées en les regroupant à un niveau plus élevé peut rendre le registre des activités de traitement plus facile à naviguer et à maintenir. La granularité dépend de la complexité de l'activité et de l'exposition au risque et peut varier au sein d'une même organisation selon les fonctions. Par exemple, le marketing peut exiger une vue plus détaillée que les activités d'approvisionnement. En le combinant avec le modèle de données de l'organisation, il peut apporter une vue riche et holistique, sans pour autant se perdre dans les détails.

De plus, la quantité d'information consignée dans le registre des activités de traitement et la fréquence de révision peuvent varier en fonction du niveau de risque. Les activités peu risquées peuvent par exemple ne consigner que les informations requises par la loi et être revues tous les 2–3 ans. À l'inverse, les activités à risque élevé, comme le développement d'une IA, celles où l'environnement est particulièrement dynamique, ou celles critiques pour la stratégie commerciale peuvent faire l'objet de revues plus poussées et fréquentes.

b) Adopter une approche top-down

Standardiser les entrées dans le registre des activités facilite la consolidation, permet de partager une vision commune des concepts, et accélère les processus de maintenance et de

revue. Il convient pour cela de prendre le temps de revoir l'ensemble des activités de traitement et de créer à partir de cela une taxonomie de tous les concepts clés de protection des données propre à l'organisation. Cette taxonomie peut alors être utilisée comme données de référence et faciliter la saisie et la mise à jour.

c) Automatiser

Automatiser les entrées dans le registre des activités de traitement en le connectant à d'autres sources de données permet de réduire les efforts nécessaires à sa mise à jour. Par exemple, il peut être relié aux analyses d'impact, à l'inventaire des applications informatiques, au modèle de données et/ou à la base de données des contrats. Il est illusoire de vouloir automatiser entièrement un registre des activités de traitement. Cependant, cela peut permettre de focaliser les ressources là où elles ont une véritable valeur ajoutée, en supervisant ces modifications et en les interprétant.

d) Responsabiliser

Assigner des responsabilités là où les activités sont menées et ne pas chercher à centraliser la tenue du registre des activités de traitement, permet d'en améliorer la pertinence et de mieux répartir la charge de travail pour le maintenir à jour. En investissant dans la communication, la formation et l'implication des collaborateurs à travers l'ensemble de l'organisation, le registre des activités peut devenir un exercice collectif, voire gratifiant pour l'organisation.

V. Conclusion – Par où commencer ?

Obtenir un registre des activités de traitement mature qui apporte autant de bénéfices qu'il ne demande d'efforts, ne se fait pas en un jour. Cela exige beaucoup de réflexion, d'efforts et surtout de temps. Pour ne pas se laisser submerger par l'ampleur de la tâche et se décourager face à la résistance de la direction et des collaborateurs qui y verront avant tout une occasion de leur créer du travail, voici quelques astuces pour démarrer :

- Visualiser le registre des activités de traitement « idéal », proportionnel et adapté à la taille, à la complexité et à la stratégie de l'organisation, mais ne pas le communiquer largement ni fixer d'échéance – cela permettra de ne pas se perdre en cours de route, de connaître les priorités, tout en évitant de se mettre une pression inutile et de « vendre du rêve ». Cette vision pourra bien entendu évoluer au fil du temps en fonction des changements législatifs, technologiques ou organisationnels, internes ou externes à l'organisation.

- Évaluer en toute honnêteté le ratio coûts/bénéfices actuel du registre des activités de traitement, en analysant son contenu, les outils, le processus et la gouvernance en place – cela permet de connaître le point de départ et d'identifier les failles et l'étendue du travail à faire.
- Commencer petit, efficace et surtout visible, puis continuer à livrer des améliorations de manière régulière et agile – cela permet de progressivement gagner en visibilité, d'augmenter l'implication des collaborateurs et de sécuriser le soutien hiérarchique quand le moment sera venu de migrer ou de mobiliser un programme de plus grande ampleur.

L'élaboration d'un registre des activités de traitement a pu s'apparenter à un sprint au moment de l'entrée en vigueur du RGPD ou de la LPD. Maintenant qu'il est en place, le rendre véritablement utile et efficace s'apparenterait davantage aux 10.000 pas par jour : un effort modéré et constant qui permet de garder un dispositif en bonne santé et résilient.

Proposition de citation : Elodie Pierloot, Le registre des activités de traitement, un outil de pilotage essentiel, 17 avril 2024 *in* www.swissprivacy.law/294