AVIS D'EXPERT

PROVADYS - INFORMATION SECURITY

Anne LUPFER est experte en gestion des risques et mise en œuvre de la sécurité de l'information.

Liste CNIL des traitements éligibles au PIA, Qu'en est-il vraiment ?

Connue sous le nom de *Privacy Impact Assessment* (PIA), *Data Privacy Impact Assessment* (DPIA) et en français, Analyse d'Impact relative à la Protection des Données (AIPD), cette activité bouleverse le quotidien des gestionnaires des risques, juristes, chefs de projet, sans oublier les responsables de traitements et les Délégués à la Protection des Données (DPD).

Le RGPD et la ligne directrice du G29 sur le PIA, datant du 4 avril 2017, apportent d'importantes précisions permettant, par l'identification de critères, d'arbitrer sur la nécessité ou non de conduire un PIA.

Voulant aider les responsables de traitements sur cette question épineuse, la CNIL avait annoncé la publication d'une liste de traitements pour lesquels l'exercice serait obligatoire. Les deux délibérations de la CNIL, publiées en octobre dernier, étaient donc très attendues.

Concrètement, quels sont les apports de ces publications ?

Pour une bonne part des traitements listés, la nécessité d'un PIA n'est pas une surprise, mais relève d'une simple application du RGPD par la rencontre d'au moins deux critères évidents et donnés par le texte lui-même, ou la ligne directrice du G29 sur le PIA.

Ces traitements sont ceux mettant en œuvre des données de santé dans les établissements de santé ou médico-sociaux ou des données génétiques de personnes dites vulnérables ainsi que ceux impliquant le profilage des personnes pouvant aboutir à leur exclusion de bénéficier d'un service.

Pour quelques traitements listés, déterminer l'applicabilité nécessitait d'avoir été attentif aux recommandations émises par le G29. Ces traitements sont en lien avec des activités de gestion des ressources humaines.

provadys

En voici un extrait :

- *Traitements établissant des profils de personnes physiques à des fins de gestion des ressources humaines (critères : évaluation ou notation et personnes dites « vulnérables »).*
- *Traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés (critères : personnes dites « vulnérables » et surveillance systématique).*
- *Traitements ayant pour finalité la gestion des alertes et des signalements en matière professionnelle (critères : évaluation ou notation, personnes dites « vulnérables » et collecte de données sensibles).*

Un critère commun à ces trois traitements est **la manipulation de données à caractère personnel de personnes dites « vulnérables »**. Si comme moi, vous vous inquiétez de savoir pourquoi les employés sont vulnérables, une relecture de la ligne directrice du G29 sur le PIA s'impose !

Voici le passage qui nous intéresse :

« Données concernant des personnes vulnérables (considérant 75) : le traitement de ce type de données est un critère en raison du déséquilibre des pouvoirs accru qui existe entre les personnes concernées et le responsable du traitement […].

*Peuvent être considérés comme des personnes concernées vulnérables, les enfants […], les **employés**, les segments les plus vulnérables de la population nécessitant une protection particulière […] et, en tout état de cause, toutes autres personnes pour lesquelles un déséquilibre dans la relation avec le responsable du traitement peut être identifié ».*

En somme, comme le résume très bien une collègue **: « La vulnérabilité de la personne va être reconnue lorsque sa relation avec le responsable du traitement est déséquilibrée et peut, par exemple, l'empêcher d'exercer ses droits »**.

Ces publications, un renfort décisionnel pour le responsable du traitement :

Cette liste, bien que non exhaustive, permet de remettre à plat les cas nécessitant de conduire une étude d'impact sur la vie privée.

Elle renforce le cadre décisionnel en lien avec l'activité de PIA et responsabilise les acteurs. Elle peut, dans certains contextes, être très impactante et forcer l'exercice qui aurait pu être jugé superflu. Elle peut avoir un réel impact sur la prise en charge de la conformité RGPD dans de nombreux établissements de santé qui, aujourd'hui, sont encore hésitants face à l'ampleur de la tâche.

Ce sera aussi, probablement, le cas de certaines Direction des Ressources Humaines qui auraient mal apprécié le caractère vulnérable de leurs salariés. Ces DRH sont ainsi mises clairement face à leurs obligations et responsabilités en matière de protection des données.

Notre recommandation :

L'analyse d'impact sur la vie privée étant une clé de voute dans la conformité au RGPD tant pour la mise en conformité, en particulier des nouveaux traitements, que pour en apporter la preuve (*accountability*), cette activité devrait être systématisée, itérative, documentée et totalement intégrée dans l'ensemble des processus de l'entreprise.

La conduite de PIA, dans tous les cas, aura des apports positifs pour votre conformité.

Nous vous recommandons de documenter systématiquement la prise de décision, qu'elle soit favorable ou non à la conduite un PIA. Il s'agira de présenter les arguments qui vous ont conduit à cette prise de décision et ainsi, donner la lisibilité sur les critères d'appréciation qui auront, par exemple, conduit à exempter un traitement.

Un PIA (même partiel) documenté est une première étape dans l'appréciation des risques associés à chaque traitement. Le PIA apportera, à minima, un éclairage jusqu'à vous aider dans la prise de décisions stratégiques.

Anne Lupfer
Project Lead - Information Security

À propos de Provadys :

Provadys vous accompagne sur votre conformité au RGPD. **Provadys** est une société de conseil, d'audit et de formation, en cybersécurité et protection des données, qualifiée PASSI par l'ANSSI. Nos équipes rassemblent des consultants experts en sécurité et des juristes, afin vous accompagner au mieux dans votre mise en conformité au RGPD.

Provadys rayonne partout en France, possède des bureaux à Paris, Sophia Antipolis et Nantes et compte plus de 200 clients actifs.

Provadys, **NetXP** et **Majj** entrent en négociation exclusive pour créer un leader français indépendant de la Cybersécurité, du Cloud et des Infrastructures. Ce rapprochement entre des structures qui partagent les mêmes valeurs, le même attachement à leurs collaborateurs et la même passion de leurs métiers, permettra au nouveau groupe ainsi créé d'élargir son offre de services, d'intensifier son activité de R&D et de se donner les moyens de relever les défis à venir. En unissant leurs forces, **NetXP**, **Provadys** et **Majj** vont pouvoir répondre plus rapidement aux nouveaux enjeux du marché.

Pour plus d'informations : contact@provadys.com / +33 (0)1 46 99 93 80.

provadys