AVIS D'EXPERT

PROVADYS - INFORMATION SECURITY

PCI DSS facilite-t-il la conformité au RGPD ?

En matière de protection des données, PCI DSS est un standard reconnu. Peut-on s'appuyer sur celui-ci pour adresser la conformité au RGPD ? Et si oui, dans quelle mesure ?

Introduction

Depuis le 25 mai 2018, les organisations publiques et privées qui traitent des données à caractère personnel doivent appliquer le Règlement Général sur la Protection des Données (RGPD), entré en vigueur à cette date, dès lors qu'elles sont établies sur le territoire de l'Union européenne ou que leurs activités ciblent directement des résidents européens.

Les entreprises manipulant des données de carte bancaire (entrant dans la définition de données à caractères personnelles (DCP) introduite par le RGPD) et devant appliquer le standard PCI DSS doivent désormais être également conformes au RGPD.

PCI DSS ?

Toute entreprise manipulant des données de carte bancaire peut, par le biais contractuel, se voir contrainte à se conformer à PCI DSS. C'est un standard évoluant depuis 2004, établi par les grandes marques de l'industrie des cartes de paiement et géré par le Conseil des normes de sécurité PCI (PCI SSC), dans le but de réduire les compromissions (massives) de données de carte bancaire.

Ce standard ne contient pas moins de 250 exigences et est un des textes les plus éprouvés en matière de sécurité des données.

Les deux textes **ont pour objectif commun de protéger des données**. Pour une entité déjà conforme PCI DSS, il est alors très tentant d'appliquer les mesures déjà mises en œuvre pour la sécurité des données de carte bancaire à toutes les données personnelles traitées. Il apparait, en effet, que de nombreux parallèles peuvent être faits.

Des mesures transposables

La sécurité des données voulue par les deux textes passe par les incontournables principes de la sécurité de l'information, qu'ils soient techniques ou organisationnels.

Le RGPD impose de sécuriser les traitements à la hauteur des risques pour les personnes concernées par les données. Pour garantir un niveau de sécurité adapté, des mesures telles que la pseudonymisation et le chiffrement des données à caractère personnel peuvent s'avérer nécessaires. Ce niveau de **confidentialité de la donnée** est imposé naturellement par PCI DSS aux données de carte bancaire. Les moyens techniques mis en œuvre pour rendre illisibles ces données de carte ainsi que pour chiffrer les flux transitant par des réseaux ouverts peuvent alors très bien être étendus à toute donnée à caractère personnel.

Ce n'est bien sûr qu'un exemple. Il serait aussi possible d'aborder le **maintien dans le temps** des mesures, le processus de **notification** en cas d'incidents de sécurité touchant les données concernées, ou encore la **surveillance des accès**, thèmes présents dans les deux textes bien que dans des mesures différentes. Et il y a d'autres points communs !

Attention cependant à ne pas perdre de vue l'objectif final du RGPD : **renforcer les droits des citoyens européens vis-à-vis de leurs données personnelles**. Et cela comprend leur disponibilité et leur intégrité alors que PCI DSS se focalise uniquement sur la Confidentialité.

Un périmètre plus large

Alors que PCI DSS demeure un référentiel essentiellement technique (malgré quelques mesures organisationnelles comme la gestion des ressources humaines et des sous-traitants, ou encore le processus de notification aux marques de cartes en cas d'incidents de sécurité existent), le RGPD nécessite quant à lui une **gouvernance à plus grande échelle**, impliquant très fortement l'ensemble des directions de l'entreprise (directions juridiques, métiers et IT) du fait de la portée de son champ d'application beaucoup plus vaste et transverse que PCI DSS.

Une grande partie du texte est en effet consacrée à la mise en place de mesures relatives aux **droits des personnes** (recueil du consentement libre et éclairé, droit d'accès, droit de rectification, droit à l'effacement, droit à la limitation du traitement, droit à la portabilité des données, et droit d'opposition), aspect totalement absent de PCI DSS.

Conclusion

Le socle de mesures techniques et organisationnelles en place pour PCI DSS peut être un véritable facilitateur pour la mise en place du RGPD. Cependant, PCI DSS ne sera pas utile dans le cadre des mesures relatives à l'exercice des droits des personnes.

Plus généralement, une entreprise soumise à plusieurs textes à tout intérêt à mutualiser au maximum les efforts et à capitaliser sur les processus en place pour adresser les différentes conformités voire à initier un système de management de la conformité intégrant l'ensemble des obligations de l'entreprise. Les particularités de chaque texte sont à prendre en compte. Une **analyse détaillée** est alors nécessaire.

Eliot Chauvineau – Consultant sécurité junior

A 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 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, 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.

www.netxp.fr | www.provadys.com | www.majj.fr

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