La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

RGPD

Vue d'ensemble

Vous avez peut-être entendu parler d'une nouvelle loi appelée RGPD ou du Règlement Général sur la Protection des Données. Cette loi a été élaborée par l'Union européenne et entrera en vigueur le 25 mai 2018. Elle s'applique à toute organisation qui traite les informations personnelles de tout résident de l'Union européenne (UE), quel que soit l'endroit dans le monde où se trouve cette organisation. La RGPD exige que les organisations préservent la confidentialité et la sécurité des informations personnelles des résidents de l'UE. Afin de garantir la conformité avec la RGPD, les principes clés doivent être compris et mis en œuvre.

Les gens ont droit à une vie privée. Les organisations doivent respecter leur vie privée en limitant les données personnelles qu'elles collectent et traitent à leur sujet et en sauvegardant ces données. Les obligations de confidentialité s'appliquent à toute information, soit seule, soit utilisée avec d'autres informations, pouvant identifier une personne vivant dans l'Union européenne. Ces informations peuvent être des adresses, des numéros de passeport, des numéros de permis de conduire, des données financières, des données biométriques, des affiliations syndicales, des antécédents médicaux, des données de localisation ou des informations relatives à l'orientation sexuelle, religieuse ou politique. Le règlement s'applique à une «personne physique», c'est-à-dire un individu vivant. Voici quelques-uns des principaux principes de la RGPD qui devront être suivis:

Les données personnelles des individus doivent être traitées légalement, équitablement et de manière transparente.

Les gens doivent être informés de ce qui est collecté et dans quel but.

Les données personnelles doivent être collectées à des fins spécifiques, explicites et légitimes. Elles ne doivent pas être utilisées pour d'autres raisons qui entrent en conflit avec ces objectifs.

Les données personnelles ne doivent être conservées et traitées que le temps nécessaire à cette fin au maximum.

Les données personnelles doivent être tenues à jour et exactes.

Les personnes ont le droit de recevoir une copie de leurs données ou peuvent demander que leurs données personnelles ne soient plus utilisées, ou dans certains cas, supprimées intégralement.

Les organisations doivent mettre en œuvre des mesures de sécurité appropriées pour protéger les données personnelles contre la destruction, la perte, l'altération ou la divulgation accidentelle ou illégale.

En outre, les organisations doivent veiller à ce que tout le personnel chargé des données personnelles soit correctement formé à la sécurisation et à la protection de ces données.

Les mesures de protection mises en place pour sécuriser les données personnelles doivent assurer un niveau de protection adapté à la nature sensible des données. Au fur et à mesure que le risque associé aux données augmente, l'effort et le coût des mesures visant à protéger les données devront l'être également. Ces mesures devraient être régulièrement examinées et mises à jour, le cas échéant. Des dossiers bien documentés sur les décisions et les mesures de confidentialité et de sécurité aident à démontrer la conformité aux exigences. En outre, les organisations sont légalement tenues d'utiliser des mesures, telles que des contrats et des contrôles préalables, pour protéger les données personnelles lors de leur transfert à des tiers externes ou en particulier à des parties extérieures à l'Union européenne. Enfin, dans le cas d'une violation de données personnelles, les organisations doivent signaler la violation dans les 72 heures après en avoir pris connaissance. L'incapacité des organisations à se conformer à la RGPD peut entraîner des amendes pouvant aller jusqu'à 4% de leurs revenus globaux, faisant de la RGPD l'une des réglementations mondiales les plus coûteuses financièrement au monde.

Version Française

La société Pélissier & Partners spécialiste en Intelligence économique a été fondée sur une expérience de plus de quinze ans dans le domaine de la recherche d'information et de la cybersécurité dédiées aux dirigeants d'entreprises suisses.

Editeur invité

Brian Honan *est le PDG de BH Consulting, une société indépendante de conseil en cybersécurité et protection des données basée à Dublin en Irlande. Brian a été conseiller spécial du Centre de cybercriminalité d'Europol (EC3), fondateur du premier CERT en Irlande et membre du comité consultatif de plusieurs sociétés de sécurité innovantes. Vous pouvez trouver Brian sur* www.linkedin.com/in/brianhonan ou Twitter @brianhonan.

Sources

Vue d'ensemble de la RGPD pour les individus et les organisations : http://gdprandyou.ie

Le règlement RGPD : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679

Traductions et archives OUCH ! : https://www.sans.org/u/D88

Comité de rédaction : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Traduit par : Marilyn Combet