Les entreprises ne sont pas prêtes pour la nouvelle législation européenne sur la protection des données | Denis JACOPINI

Les entreprises ne sont pas prêtes pour la nouvelle législation européenne sur la protection des données

Varonis a mené une enquête en mars auprès des informaticiens professionnels participant au CeBIT, le plus grand salon IT d'Allemagne, afin de recueillir leur opinion sur la nouvelle réglementation régissant la protection des données qui doit entrer en vigueur cette année ou l'année prochaine. Le constat est sans appel : les entreprises ne sont pas prêtes pour la nouvelle législation européenne sur la protection des données. Les professionnels interrogés par Varonis ne pensent pas que leurs entreprises soient en mesure de respecter les délais imposés par l'UE pour la notification des violations de données.

Il ressort de cette enquête que 80 % des personnes interrogées pensent qu'une banque sera très probablement la première entreprise à être frappée par l'amende maximale de 100 millions d'euros pour non-respect de la réglementation européenne sur la protection des données. À la question concernant le pays le plus probable de cette banque, les répondants indiquent l'Allemagne (30 %), les États-Unis (28 %) et 22 % mentionnent un autre pays européen. 48 % seulement des personnes interrogées pensent que leur entreprise pourrait signaler une violation dans le délai obligatoire de 72 heures.
Seuls 31 % disposent d'un plan leur permettant de se conformer à la nouvelle législation et seulement un tiers des personnes enquêtées a mis en place les processus et la technologie nécessaires pour empêcher leur entreprise de se voir infliger une amende importante dans le cadre de cette loi. 71 % des répondants sont incapables de dire ce que les entreprises doivent faire pour se conformer à la nouvelle réglementation.
Seuls 22 % des répondants savaient que l'amende maximale prévue par la nouvelle législation est de 100 millions d'euros, 41 % pensaient qu'elle ne serait que de 10 millions d'euros et 32 % l'estimaient à 1 million d'euros, avec un nombre réduit de personnes interrogées croyant qu'elle pouvait s'élever à un milliard d'euros. Un tiers a déclaré que la réglementation européenne sur la protection des données entrera en vigueur en 2015, 28 % ont indiqué que tel serait le cas en 2016, 7 % estiment que la loi ne verra jamais le jour et 32 % des personnes interrogées ont dit ne pas savoir quand la loi entrerait en vigueur.
« Nous pouvons attendre une refonte majeure de la loi européenne sur la protection des données au cours des prochains 12 à 24 mois », déclare David Gibson, vice-président du marketing de Varonis. « Les amendes devraient s'élever à 2 % du revenu annuel avec un plafond de 100 millions d'euros ou de dollars pour la non-protection des données personnelles des citoyens européens. Il pourrait également y avoir un nombre important de plaintes individuelles en plus des amendes et les sommes mises en jeu pourraient donc représenter des coûts substantiels, même pour les grandes entreprises. La nouvelle loi marquera aussi le passage d'un environnement autoréglementé à un régime d'application obligatoire qui aura une incidence sur toute entreprise stockant des informations d'identification personnelle concernant les citoyens européens (y compris sur les sociétés américaines menant des activités dans l'UE). Les entreprises doivent être préparées à protéger les données de leurs clients et prouver qu'elles le font avec le soin approprié, rendre compte de toute violation et supprimer les données à la demande des citoyens de l'UE. »
« Compte tenu de la vaste portée de la nouvelle réglementation et de l'importance accrue des amendes, cette enquête révèle des inquiétudes très importantes quant aux efforts que les entreprises sont prêtes à fournir pour se conformer aux conditions de la réglementation et gérer les scénarios de violation de données », indique Mark Deem, partenaire de Cooley LLP au Royaume-Uni. « En fait, l'échelle des amendes potentielles sera plus proche de celles infligées pour corruption ou violation antitrust, ou dans le secteur des services financiers. La conformité en matière de protection des données sera tout aussi importante que la conformité aux réglementations de la FCA. Même si la législation n'entre pas en vigueur avant 2017, un travail considérable doit être accompli par ceux qui souhaitent offrir des biens et des services aux habitants de l'UE et s'assurer qu'ils se trouvent dans la meilleure situation possible pour respecter la loi. »
Varonis propose 7 conseils pour garantir la conformité des données non structurées et permettre aux entreprises de se préparer à la réglementation européenne sur la protection des données :

1. Minimiser la collecte des données : la proposition de loi de l'UE comporte de fortes exigences en ce qui concerne la limitation des données recueillies auprès des consommateurs.

2. Favoriser le signalement des violations de données : la notification des atteintes à la protection des données constitue une nouvelle exigence que les entreprises européennes devront respecter.

3. Conserver les données avec attention : les règles de minimisation de la nouvelle loi concernent non seulement l'étendue des données collectées, mais aussi leur durée de rétention. En d'autres termes, une entreprise ne doit pas stocker les données plus longtemps que nécessaire aux fins prévues.

4. Nouvelle définition des identifiants personnels : l'UE a étendu la définition des identifiants personnels et ce changement s'avère important parce que les lois de l'UE portent sur la protection de ces identifiants.

5. Employez un langage clair : il faudra à une entreprise le consentement préalable et explicite des consommateurs lors de la collecte des données.

6. Bouton d'effacement : le « droit d'effacement » signifie qu'en cas de retrait du consentement accordé par les consommateurs, les sociétés devront supprimer les données concernées.

7. Le Cloud computing n'échappe pas à cette nouvelle loi de l'UE, car celle-ci suit les données.

Méthodologie de l'enquête
Les 145 personnes interrogées constituent un échantillon représentatif des participants du plus grand salon informatique d'Allemagne qui a compté 221 000 visiteurs en mars 2015. Parmi les répondants, 16 % sont issus de banques allemandes, 3 % de banques américaines, 3 % de banques européennes, 45 % d'entreprises allemandes hors du secteur financier, 26 % d'entreprises européennes hors du secteur financier et 7 % d'entreprises américaines.
