Protection des données personnelles et contrôles de la CNIL : comment s'y préparer ?

Dans un contexte de cyber-attaques répétées et alors que tout internaute peut porter plainte auprès de la CNIL (Commission Nationale de l'Informatique et des Libertés) concernant le traçage sur Internet, la protection des données liées à la vie privée est un enjeu critique pour les entreprises de tout type et de tout secteur.

Confiance et conformité ne sont plus un luxe réservé aux grands acteurs du numérique. La réglementation s'adapte, les contrôles se multiplient, les sanctions se durcissent… mais de quoi s'agit-il ? Comment s'y préparer ? Comment s'assurer de sa conformité ? et quid de la gestion des cookies ?

Les contrôles de la CNIL, kesako ?

À l'heure actuelle, nous n'avons d'autre choix que d'améliorer la protection de la vie privée au sein de nos organismes et la CNIL est là pour nous contrôler. Pour ce faire, cette dernière dispose d'un service dédié, composé de juristes et d'informaticiens contrôleurs, ayant pour mission de vérifier la conformité des organismes à la loi « Informatique et Libertés ». Une procédure pouvant donner lieu à des sanctions.

Si l'on peut penser que la crise a contraint la CNIL à réduire le rythme de ces actions de régulation, il n'en est rien, celle-ci ayant désormais recours aux contrôles à distance ou sur convocation.
Pour déterminer les entreprises à examiner, elle se base sur plusieurs entrées : une plainte (d'où l'importance d'identifier ses axes d'amélioration pour éviter les griefs) ; un traitement visible que la commission aurait identifié comme sensible (d'où la nécessité de s'assurer en priorité de la conformité des éléments facilement consultables, comme les registres, les mentions d'information et les analyses d'impact) ; et son programme annuel.

Sur ce dernier point, les priorités affichées par la CNIL en 2021 sont la cybersécurité des sites web français, la sécurité des données personnelles, notamment de santé, et l'utilisation des cookies et autres traceurs web. Dans un contexte où les sanctions mises en œuvre augmentent, il est plus que jamais essentiel de se prépare et d'anticiper au maximum d'éventuels contrôles.

Se préparer et s'assurer de sa conformité : par où commencer ?

Lorsque la CNIL contrôle un organisme, ce dernier a peu de temps pour répondre. L'anticipation est donc clé. Comment s'organise-t-on ? Quelle est la cellule de crise (rôles, responsabilités, salles…) ? Quels sont les points les plus sensibles dans l'organisme ? Quelles sont les règles à respecter pour

communiquer les preuves ? Quel est le bon vocabulaire à adopter ? Autant de questions auxquelles il est préférable de répondre en amont. S'il est absolument essentiel de se montrer transparents et coopératifs, le meilleur moyen pour se tenir prêt est de réaliser une simulation de contrôle. De quoi juger grandeur nature de l'efficacité de la méthodologie choisie.

Pour aller plus loin, il est également possible de réaliser des audits, de l'organisme en lui-même ou bien d'un ou plusieurs traitements. Un organisme met en œuvre, de manière formelle ou non, des processus qui sont liées à la protection de la vie privée et dont il est possible d'évaluer leur maturité. Après avoir attribué pour chaque activité son niveau de maturité, il s'agira de définir les prochaines étapes pour que tous les processus de l'organisme soient continuellement optimisés.

Avec la vision par traitements, il est possible d'évaluer la conformité de chacun d'eux en se basant sur la doctrine de la CNIL. Il s'agit alors de réaliser une étude juridique du respect des principes fondamentaux de protection de la vie privée et une étude technique des risques liés à la sécurité des données. L'idée est d'identifier ce qu'il peut se passer en cas de disparition, modification non désirée ou accès non autorisé à des données personnelles.

Après avoir défini les bonnes pratiques à mettre en œuvre – en termes de sensibilisation, d'authentification, d'habilitations, de journalisation et de gestion des incidents, de postes de travail, d'informatique mobile… – cet audit donne lieu à un plan d'action.

Quid de la gestion des cookies et autres traceurs web ?

Depuis le 1er avril 2021, la CNIL impose de nouvelles règles sur l'utilisation des cookies. Désormais, poursuivre sa navigation sur un site sans avoir validé l'utilisation de ces traceurs numériques n'a plus valeur d'accord tacite. Les organismes exploitant des cookies doivent ainsi être en mesure de fournir, à tout moment, la preuve du recueil du consentement libre, éclairé, spécifique et univoque de l'utilisateur. Quant aux preuves de consentement, l'expérience montre qu'un registre est complexe à produire et à exploiter, et qu'une description du mécanisme de gestion des données pourrait être préférable.

Ces derniers mois, la CNIL multiplie les contrôles en ce sens. Or, la gestion des cookies fait partie des points visibles, facilement contrôlables. Si les responsabilités sont partagées entre l'éditeur du site et l'émetteur des cookies selon le type de traceur déposé, les sanctions encourues peuvent aller jusqu'à plusieurs dizaines de millions d'euros. Une loi est par ailleurs en cours de discussion pour permettre à la commission d'accélérer ses processus en termes de sanctions.

Pour les éviter et être en conformité, il s'agit dans un premier temps d'identifier les cookies existants (les lister, les catégoriser et vérifier leur pertinence) avant d'informer les utilisateurs de manière intelligible. Nous recommandons pour ce faire la mise en place d'un bandeau cookies redirigeant vers une page dédiée à la politique de gestion des données. Il est également nécessaire de recueillir leur consentement en leur donnant la possibilité d'accepter, de refuser ou de personnaliser leur choix, ce sans orienter leur réponse, mais aussi de leur fournir un moyen de retirer leur consentement à tout moment.

Autant de bonnes pratiques qui permettront aux entreprises tout à la fois d'éviter les potentielles sanctions, d'améliorer la maitrise de leur système d'information, mais aussi et surtout d'apporter la transparence et la confiance, aujourd'hui essentielles, à leur clients, partenaires et collaborateurs.