RGPD : Le 25 mai 2018 est passé et vous n’êtes pas encore en conformité avec le règlement ? Que risquez-vous vraiment ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	RGPD : Le 25 mai 2018 est passé et vous n’êtes pas encore en conformité avec le règlement ? Que risquez-vous vraiment ?				

Comme l'a encore indiqué récemment Isabelle Falque-Pierrotin, la présidente de la CNIL, « Le 25 mai ne sera pas une date couperet pour les sanctions » contre entreprises, administrations et associations concernées par la nouvelles réglementation européenne sur la Protection des Données à caractère personnel.

24 MAI 2018 23h59

La France est déjà bien endormie et, mis à part quelques rares entreprises Européennes ayant déjà entamé une démarche de mise en conformité depuis l'ancienne réglementation relative à la protection des données à caractère personnel, des millions d'entreprises n'ont absolument aucune conscience du top départ de nouvelles obligations et sanctions applicables en référence au RGPD.
Plus que quelques secondes avant le 25 mai 2018 0h00 et des milliers d'entreprises, administrations et administrations sont en stress à la suite des millions de messages alarmants envoyés ces derniers mois sur les obligations à mettre en place au plus tard à cette date limite.

DÉMARCHE LONGUE MAIS PAS FORCÉMENT COÛTEUSE

Cette démarche est longue car elle n'a pas de fin et « **on ne devient pas conforme avec le RGPD** » (puisqu'il n'existe pas de référentiel et que le contexte à analyser est sans cesse en mouvement) mais « **on met en place une démarche de mise en conformité avec le RGPD** ». Cette démarche doit être prise en compte et s'intégrer dans la continuité de l'activité de l'organisme, sans la révolutionner, mais juste l'adapter à des obligations vieilles de plus de 40 ans, la Loi n° 78-17 du 6 janvier 1978 dite Loi Informatique & Libertés ou aussi Loi I&L.
De plus, cette démarche n'est pas forcément coûteuse, car elle dépend avant tout de la manière dont vous souhaitez y participer en mouillant le maillot. Bien que recommandée, la contractualisation d'un service d'accompagnement par un professionnel n'est nullement obligatoire. Par contre, nous vous conseillons la mise en place de démarches de formations qui seront utiles à la fois pour acquérir une autonomie et profiter de la prise en charge financière des formations permettant justement d'acquérir cette autonomie. Des aides financières existent pour ça. Rapprochez-vous de votre comptable ou de votre organisme collecteur de vos charges sociales.

A PARTIR DU 25 MAI 2018 0H00

La CNIL a aujourd'hui conscience qu'au lieu de mettre en place les nouvelles mesures de conformité avec le RGPD depuis le 27 avril 2016 comme cela avait prévu, avec la possibilité d'appliquer les nouvelles sanctions maximales (20 millions d'euros ou 4% du Chiffre d'Affaire mondial) le 25 mai 2018, une très grande partie des entreprises, administrations et associations se sont réveillées pour la plupart au mois de mars, avril et même mai 2018 pour certains dans le but d'initier cette longue démarche réglementaire.
Même si vous avez très peu de risque d'être contrôlé **LE** 25 mai 2018, avec quelques années d'expérience et le rapports d'activités de la CNIL de ces dernières années en main, ne pas avoir entamé de démarche de mise en conformité à partir de cette date vous expose toutefois à quelques situations dont le risque ne peu être négligeable :

• En 2017, 8360 plaintes ont été déposées à la CNIL. 100% des plaintes ont été prises en compte, c'est-à-dire qu'elle a demandé des explications à chacun des organismes concernés qui ont du montrer patte blanche. **En raison d'un salarié mécontent ou licencié, d'un concurrent peu diligent ou d'un vif ennemi, vous pouvez facilement vous retrouver à devoir donner des explications à la CNIL**. Il vaut mieux que le jour où ça vous arrive, vous ayez déjà entamé une démarche de mise en conformité et que vous soyez diligents vis-à-vis de la CNIL, sinon, vous pourriez bien voir arriver chez vous ses contrôleurs, assermentés avec pouvoir de sanctionner sans le moindre jugement (la CNIL étant une autorité administrative indépendante comme l'ARCEP et une cinquantaine d'autres en France) ;

• En 2017, 62% des contrôles ont été effectués à l'initiative de la CNIL, notamment au vu de l'actualité. Ceci signifie que les contrôles ne dépendent pas du hasard ni de votre position géographique dans une ville ou le numéro de votre rue, mais **les contrôles de la CNIL dépendent de faits liés à des risques bien réels constatés auprès d'autres organismes ayant la même activité que la votre** ;

• En France en 2017, selon Symantec, il y a eu 19 millions de victimes de la cybercriminalité. Parmi ces victimes, il n'est pas rare de voir des entreprises, des administrations ou des associations qui ont subit un vol de données. A partir du 25 mai 2018 à 0h00, **tous ces organismes doivent signaler dans les 72 heures à la CNIL qu'ils ont été victimes d'un vol de données**. Il est évident que pour la plupart des fuites de données, la CNIL demandera des explications à leur détenteur et responsable de leur confidentialité. Vous devrez là aussi donner des explications à la CNIL au sujet de l'absence de démarche de mise en conformité avec la CNIL ;

• Enfin, parmi les grands changements du RGPD nous trouvons la suppression des déclarations préalables. C'est-à-dire qu'avant le 25 mai 2018 0h00 vous devez toujours avoir des démarches déclaratives de vos traitements de données à caractères personnel, à partir du 25 mai 2018, vous devez avoir une démarche de « privacy by design » (protection de la vie privée obligatoire) et devrez rendre compte à la CNIL de vos démarche seulement sur demande de sa part. Cependant, **tous les employés de la CNIL qui étaient chargés de traiter les déclarations pourraient bien se voir affectés aux contrôles**, renfonçant ainsi les capacités de contrôle de la CNIL pour en augmenter leur volume. Moins de formalités à la CNIL pour avoir plus de temps pour les contrôles ?

QUE VA CHANGER LA MISE EN APPLICATION DU RGPD

Le Règlement Général sur la Protection des Données est une poursuite de la Loi n°78/16 Informatique & Libertés avec toutefois quelques mesures en faveur des individus mais aussi quelques nouveautés parmi lesquelles :

• Conséquence n°1 : **Pas en conformité avec le RGPD = fin du travail avec ou pour les administrations** ou sous-traitants d'administrations. En effet, toutes les administrations, obligées de ce conformer à ce règlement, devront désigner un délégué à la Protection des Données (DPD en français ou DPO Data Protection Officer en anglais). Le DPD aura obligation d'entamer une démarche de mise en conformité auprès de son organisme mais aussi auprès de tous les sous-traitants de l'organisme, sous peine de ne pas être lui même en règle; Tous les organismes qui travaillent avec les administrations et leurs sous-traitants devront donc obligatoirement, pour prétendre se positionner sur des marchés publics, se mettre en conformité ;

• Conséquence n°2 : **La mise en application de sanctions bien plus importantes** (20 millions d'euros ou 4% du chiffre d'affaire en lieu et place de 150 000 euros ;

• Conséquence n°3 : Désormais plus de 80% des utilisateurs d'Internet déclarent être soucieux de la protection mise en place par les sites Internet et les fournisseurs autour de leurs données personnelles. Beaucoup ne veulent plus communiquer leur vrai nom, leur adresse perso ou leur numéro de téléphone perso. Beaucoup utilisent des pseudos ou des adresses e-mail poubelle pour ne pas risquer de se voir polluer ou pire pirater leur boite. Ne pas montrer auprès de ses contacts qu'une démarche de mise en conformité est en place aboutira tôt ou tard à **une fuite des clients ou adhérents vers d'autres organismes** affichant et prouvant leur respect des droits et libertés des personnes ;

• Conséquence n°4 et pas des moindres : **Vous devrez obligatoirement obtenir le consentement de quelqu'un avant de traiter ses données**. L'obligation du consentement des propriétaires de données personnelles n'ayant pour la plupart du temps jamais été sollicité par les organismes, c'est la raison pour laquelle pour pouvez recevoir des e-mails vous demandant si vous êtes toujours d'accord pour recevoir des informations de la part d'un contact, fournisseur, ou tout simplement parfois un pollueur… Un bon moyen pour réduire le nombre de mails dans sa boite de réception mais aussi de faire le ménage dans les coordonnées utilisées par les expéditeurs ;

• Conséquence n°5 : Si vous êtes victime d'une fuite de données et qu'une personne victime de cette fuite décide de vous attaquer, vous êtes pénalement responsable. Votre niveau de responsabilité et le montant des sanctions appliquées seront immédiatement en corrélation avec les démarches que vous avez déjà accomplies. Au plus vous prouvez votre bonne fois par une prise en prise en compte (par le biais de formations et de démarches internes) des démarches visant à protéger les libertés fondamentales et individuelles de vos contacts, au plus la CNIL sera bienveillante. Au plus vous ferez preuve de mauvaise foi sans apporter le moindre élément montrant la prise en compte de vos obligations relatives au RGPD, plus forte sera la sanction.

• Conséquences n°6 : Un nouveau droit à la portabilité, la majorité numérique et un droit à l'effacement apparaissent également.

CONCLUSION

Vous l'autre compris, à partir du 25 mai 2018 0h00, vous n'allez pas voir débarquer chez vous les militaires, et la vie de votre organisme ne va pas s'en trouver bloquée, cependant, les risques de piratage, de contrôle de la CNIL et les montants des sanctions augmentant de manière significative, même si votre démarche de mise en conformité n'est qu'à ces débuts, à votre rythme, poursuivez-la. Prenez contact avec un expert en RGPD, participez à une formation, mettez en application les 6 étapes recommandées par la CNIL (https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes), faites ce que vous voulez mais faites au moins quelque chose.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?
Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.
« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :

Quelques articles sélectionnés par nos Experts :
Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

Source : *RGPD : « Le 25 mai ne sera pas une date couperet pour les sanctions », assure la CNIL – Les Echos*