Vous avez dit RGPD ?

La réglementation sur la protection des données personnelles a presque 40 ans !

En France, c'est en 1978 qu'une réelle prise de conscience s'opère concernant les risques éventuels liés aux données informatiques. C'est par la Loi du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, loi modifiée par la loi du 6 Août 2005 relative à la protection des personnes physiques concernant les traitements de données à caractère personnel que nous prenons enfin conscience des risques liés à nos données. Le Conseil de l'Europe rédige le traité N°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, traité ouvert à la signature des Etats membres et à l'adhésion des Etats non membres le 28 janvier 1981. Depuis cette date de nombreuses directives, lois, décrets, propositions sont intervenus jusqu'au Règlement Européen du 4 Mai 2016 qui est entré en application le 25 Mai 2018.

La réglementation n'a pas énormément changé entre le 24 et le 25 Mai, l'esprit de la loi est globalement repris par la nouvelle réglementation sur la protection des données personnelles (RGPD). Les entreprises ne sont donc pas réellement plus en défaut de conformité que la veille seul le niveau des sanctions passe de 300 000 € à 20 Millions d'€uros et jusqu'à 4% du chiffre d'affaire du groupe, ceci est certainement la raison d'un vent de panique.

Chef d'entreprises ou pas, la réglementation est avant tout une mesure permettant de nous protéger face aux menaces grandissantes d'attaques informatiques, vols de données, commercialisations illicites de nos données, nous devons convenir que la cyber sécurité est maintenant l'affaire de tous.

En France, la législation sur la protection des données est gérée par la Commission Nationale Informatique et Libertés (« CNIL »). La Cnil n'est pas seulement un organisme de contrôle, elle fournit également des informations aux personnes sur leurs droits, elle autorise ou non le traitement de données personnelles lorsque des risques résiduels sont encore présents à l'issue de l'analyse d'impact sur la vie privée réalisée par l'entreprise pour des traitements de données sensibles ou à grand échelle.

La CNIL procède également à des contrôles à distance, c'est pourquoi il est urgent et primordiale pour les entreprises ayant des sites internet de mettre rapidement leurs sites en conformité avec la réglementation en indiquant les mentions d'informations sur le traitement des informations, la durée de conservation, droit à l'effacement, à la limitation, la portabilité, retirer son consentement, etc…. Il faut aussi procéder à la mise en œuvre du recueil du consentement express du prospect qui souhaite recevoir vos informations commerciales ou vos newsletters avec enregistrement de la preuve de l'accord.

Et les Cookies sur nos sites internet ?

Lorsque que l'éditeur du logiciel détermine les moyens et finalités du traitement réalisé par la collecte de données via des cookies il est considéré comme le responsable de traitement et en ce sens il doit assumer l'ensemble des obligations de la loi et en particulier l'article 32-II (recueil du consentement et information avec moyen de s'opposer). Dans le cas ou les cookies sont utilisés exclusivement dans le cadre d'une prestation de sous-traitance un contrat doit clairement interdire à l'émetteur des cookies d'exploiter les données collectées pour son compte ou pour celui d'autrui. Les sites de commerce en ligne, les systèmes de mesures ou d'analyse d'audience sont donc concernés par ces évolutions de la réglementation et en particulier au projet de futur règlement « ePrivacy »

Le RGPD que change t-il vraiment ?

Le nouveau règlement introduit de nouveaux droits pour les individus mais aussi de nouvelles obligations pour les sous-traitants. Ceux-ci voient maintenant leurs responsabilités réellement engagées en cas de non-conformité sur la mise en œuvre d'un traitement de données personnelles. Le fournisseur n'est plus le seul à devoir assumer la responsabilité si la responsabilité de son sous-traitant est engagée. Le règlement permet une meilleure information aux personnes et le recueil et la traçabilité de leurs consentements. Le nouveau texte réglementaire permet un allègement des formalités à réaliser auprès de la CNIL mais il nécessite maintenant de tenir un registre des activités de traitements. Les principaux droits introduits par le nouveau texte sont le droit à la portabilité des données, le droit à l'effacement ou droit à l'oubli, le droit à la limitation du traitement. De nouvelles obligations voient également le jour avec l'obligation de mettre en œuvre des mécanismes et procédures permettant de démontrer le respect des règles sur la protection des données mais aussi l'obligation de mettre en place des processus permettant de tenir compte de la protection des données dès la conception des produits ou des services. La sécurité informatique est également très présente au travers la nécessité de décrire les mesures techniques et organisationnelles de sécurité mis en œuvre.

Les 8 principes de base à retenir concernant les données à caractère personnel:

La loyauté : Elles doivent être traitées d'une manière loyale (Article 6.1).

Légitimité : Elles doivent être conservées durant une durée légitime qui n'excède par la durée nécessaire pour la finalité et les exigences réglementaires. (Exemple 3 ans pour un fichier prospect)

Proportionnalité : Les données sur pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées.

Qualité : Elles doivent être exactes et tenues à jour.

Finalité : Elles sont collectées uniquement pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec les finalités du traitement. (sauf exception particulière pour la recherche scientifique)

Transparence : Le consentement de la personne concernée a été collecté ou il intervient dans le respect des obligations légales incombant au responsable de traitement, sauvegarde de la vie de la personne, exécution d'une mission de service public, légitimité de l'exécution du contrat.

Sécurité : Le responsable du traitement est tenu de prendre des mesures de sécurité physique et logiques (droits d'accès, cryptage) afin d'empêcher qu'elles soient corrompues, endommagées ou que des tiers non autorisés y aient accès. Le contrat liant le sous-traitant au responsable du

traitement comporte de nouvelles indications concernant les obligations incombant au sous traitant en matière de protection de la sécurité et de confidentialité, le sous traitant tient également un registre des traitements réalisés pour le compte de son client. **Territorialité :** Le transfert de données de données personnelles en dehors de UE est soumis à une réglementation stricte avec nécessité de mettre en place des règles internes d'entreprises (BCR) ou des clauses contractuelles types approuvées par la Commission Européenne sauf pour les pays reconnus adéquats par la commission.

Mais de quels traitements parle-t-on ?

Les données personnelles sont des données comportant un nom, un prénom, un numéro de téléphone, plaque d'immatriculation, adresse IP, RFID, etc … Le numéro de sécurité sociale est quant à lui une donnée personnelle sensible et la taille et le poids de la personne forment à eux deux des données de sante. Les données pouvant être rattachées à une personne sont aussi des données personnelles comme par exemple les achats, déplacement, communication, centre d'intérêts, etc…

Le nombre de traitements varie souvent entre une dizaine pour une petite société à près d'une centaine pour une collectivité locale. La comptabilité, gestion de la paie, gestion des fournisseurs, gestion des chambres d'hôtes, gestion du personnel, recouvrement, gestion commerciale, gestion des fichiers clients et prospects, gestion patrimoine, etc… sont des traitements qu'il conviendra de porter au registre des traitements.

Le principe d'«Accountability »

Il s'agit d'une obligation pour la structure de mettre en œuvre des mécanismes et procédures internes permettant de garantir le respect des règles relatives à la protection des données personnelles. Depuis le 25 mai, il n'est plus obligatoire d'informer les autorités compétentes concernant le traitement des données personnelles mais il est désormais impératif de mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires afin de prévenir tout risque lié à ces données. Cette nouvelle obligation implique bien souvent pour l'entrepreneur de revoir ses contrats, sa politique de confidentialité, de procéder à des analyses de risques, s'interroger et documenter les durées de conservations des données en s'appuyant sur le cadre légal qui entoure le traitement de données. D'autres autres points sont à prendre en compte en fonction des activités de traitements de données effectuées : vérifier l'état des données et de la documentation, implémenter une analyse d'impact sur la vie privée, la nécessité ou non de nommer un Délégué à la Protection des Données, l'enregistrement et la conservation des preuves du consentement dans le cadre du RGPD, l'intérêt légitime du traitement et la proportionnalité des données ainsi que la finalité et changement de finalité des traitements. Dans le cas d'envoi de données à l'extérieur de l'Europe il convient de vérifier les accords entre les pays et d'éventuellement nécessitant souvent la mise en place de règles entre entreprises « Binding Corporate Rules (BCRs) ».

Le « Privacy by default & by design » c'est quoi ? :

Il s'agit d'une obligation de déployer des processus permettant de prendre en compte la protection des données personnelles dès la conception d'une application ou d'un traitement. Le délégué à la protection des données ou le correspondant si vous n'avez pas de délégué trouvera sa place lors des réunions stratégiques de développement d'un nouveau produit, nouveau service, nouveau site internet en lien avec des données personnelles afin que dès la conception les principes de sécurités puissent être pris en comptes.

La désignation d'un délégué à la protection des données est-elle obligatoire ?

Le délégué à la protection des données (DPD ou DPO) est obligatoire pour les organismes publics mais pour ce qui concerne les entreprises il n'est pas toujours obligatoire. La réglementation précise que le DPD n'est pas obligatoire pour les entreprises TPE, PME de moins de 250 salariés (considérant n°13 du règlement Européen UE 2016/679) mais attention car il peut devenir très vite obligatoire même pour une société d'un ou deux salariés ! Le DPD est notamment obligatoire si vous êtes une entreprise dont l'activité de base vous amène à réaliser un suivi régulier et systématique des personnes à grande échelle ou à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et à des infractions. Même si votre organisme n'est pas formellement dans l'obligation de désigner un délégué à la protection des données, il est fortement recommandé de désigner une personne, disposant de relais internes, chargée de s'assurer de la mise en conformité au règlement européen. Afin de déterminer si le traitement qui est mis en œuvre est à grande échelle le G29 recommande de tenir compte des facteurs suivants : le nombre de personnes concernées, en valeur absolue ou en valeur relative par rapport à la population concernée ; le volume de données et/ou le spectre des données traitées ; la durée, ou la permanence, des activités de traitement des données ; l'étendue géographique de l'activité de traitement. Le choix d'un délégué à la protection des données qu'il soit salarié ou externe doit s'effectuer en adéquation avec les articles 37-38-39 du règlement européen dans lequel sont défini les qualités professionnelles nécessaires ainsi que ses fonctions et sa mission. Le DPD « est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39». Le niveau de connaissances spécialisées requis devrait être déterminé en fonction des opérations de traitement de données effectuées et de la protection exigée pour les données à caractère personnel traitées. Le DPD possède une bonne compréhension des opérations de traitement effectuées, ainsi que des systèmes d'information, une bonne connaissance des règles et procédures administratives. Il est essentiel qu'aucun des membres de l'organisme n'ait de conflit d'intérêts. Les coordonnées du DPD doivent être communiquées à l'autorité de contrôle compétente. La fonction du DPD peut aussi être exercée sur la base d'un contrat de service conclu avec une personne ou un organisme indépendant de l'organisme du responsable du traitement ou du sous-traitant. Dans ce cas, il est essentiel que chaque membre de l'organisme exerçant les fonctions de DPD remplisse l'ensemble des exigences applicables établies à la section 4 du RGPD (par exemple, il est essentiel qu'aucun des membres de l'organisme n'ait de conflit d'intérêts).

Le chemin vers la conformité ?

La première étape pratique consiste dans une séance d'information et d'échanges avec le responsable de l'entreprise (PILOTE) et les personnes concernées afin que chacun puisse apprécier le périmètre du travail à effectuer et de s'organiser (CARTOGRAPHIER). Dans un deuxième temps, parfois le même jour, des interviews sont réalisés avec les différents services, compter environ 1h à 2h pour chacun des services, ces échanges permettent l'identification et l'élaboration de la liste des traitements. Lors de l'identification, le cadre légal, les durées de conservation des données, la légitimité, etc… sont abordés. A l'issue de cette phase, il convient de s'interroger sur la nécessité ou non de pratiquer des analyses des risques simplifiées pour chaque traitement voire une analyse de la vie privée pour certains traitements (AIPD ou AIVP – GERER LES RISQUES). Les étapes suivantes seront la mise en place du registre des traitements et l'information individuelle, mise en place d'un plan d'actions, priorisation (PRIORISER), accompagnement (ORGANISER), documentation (DOCUMENTER), audit et/ou rapport annuel. Durant ces différentes phases seront pris en compte le contexte, la typologie des données, la sécurisation, menaces, vulnérabilité, les contrats, la charte informatique, les mentions légales, etc…

La réglementation ne doit pas être perçue comme une contrainte car même si elle est en est une par certains aspects elle peut-être un réel levier pour les petites et moyennes entreprises qui se mettent rapidement en conformité. En effet les TPE pourront rapidement bénéficier de l'opportunité de signer de nouveaux contrats de sous-traitance car comme vous l'avez compris les donneurs d'ordres n'ont pas d'autre solution que de choisir des entreprises en conformité avec la réglementation. La mise en œuvre du RGPD permet aussi de protéger les entreprises de la perte partielle ou totale d'activités liées à la cybercriminalité et offre un moyen efficace pour relancer nos prospects avant qu'ils ne partent aux oubliettes en raison des délais légaux d'effacement.

Mettons la conformité au service de l'entreprise et conservons la souplesse et l'agilité des petites et moyennes entreprises.

Franck DURAND, Conseil et Formation
Juin 2018
www.franck-durand.com