RGPD : réponses aux questions les plus posées

Introduction

Syntec Numérique a reçu de nombreuses questions sur le règlement général relatif à la protection des données personnelles dit « RGPD » de la part des entreprises du numérique, adhérentes de Syntec Numérique. Les réponses aux questions les plus posées sont regroupées dans cette foire aux questions (FAQ).

Cette FAQ sera alimentée au fur et à mesure par des questions susceptibles d'intéresser l'ensemble des entreprises du numérique, qu'elles soient entreprises de services du numérique, éditeurs de logiciels ou sociétés de conseil en technologies.

Table des matières

1. Comment Syntec Numérique accompagne-t-il ses adhérents ?

Syntec Numérique est mobilisé pour vous informer, vous sensibiliser et vous accompagner sur la mise en œuvre du RGPD. Cet accompagnement est articulé autour d'actions clés :

- Une rubrique dédiée au RGPD sur le site internet de Syntec Numérique
- Des documents de référence (outils, guides, etc.)
- Une collection de fiches PraTIC dédiées au RGPD
- Des conférences juridiques RGPD sur des sujets ciblés
- Des conférences web mensuelles
- Une réponse aux questions juridiques adressées à nos experts
- Un référencement des adhérents de Syntec Numérique proposant des prestations d'accompagnement dédiées au RGPD
- Une contribution aux débats et à l'élaboration des lignes directrices

2. Qu'est-ce qu'une donnée à caractère personnel, une donnée sensible et un traitement de données personnelles ?

Données à caractère personnel

Toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
Exemples : nom, numéro de carte d'identité, passeport, permis de conduire, empreintes digitales, etc.

Données sensibles ou catégories particulières de données

Traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Traitement

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction

3. Responsable du traitement, sous-traitant, personne concernée, destinataire des données, tiers, délégué à la protection des données, autorité de contrôle, qui est qui ?

Responsable du traitement	La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre. Exemples : pour une entreprise, il est incarné par un représentant légal personne physique : le Président, le Directeur Général…
Sous-traitant	La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Exemple : prestataires informatiques
Personne concernée	La personne dont les données à caractère personnel font l'objet d'un traitement de données à caractère personnel
Destinataire	La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires
Tiers	Une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel
Délégué à la protection des données	Interne ou externe, le délégué à la protection des données : - informe et conseille le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du RGPD d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données,

- contrôle le respect du RGPD, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant,
- dispense des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifie l'exécution de celle-ci,
- coopère avec l'autorité de contrôle,
- fait office de point de contact pour l'autorité de contrôle sur les questions relatives aux traitements, y compris la consultation préalable visée à

Autorité de contrôle → Une autorité publique indépendante instituée par un État membre en vertu de l'article 51 du RGPD, chargée de surveiller l'application du RGPD, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union européenne
Exemple : en France, la Commission nationale de l'informatique et des libertés (CNIL)

4. TPE/PME, êtes-vous concernées par le RGPD ?

Oui car l'application des règles relatives à la protection des données à caractère personnel ne dépend pas de la taille de l'entreprise.

Les dispositions du RGPD s'appliquent à toute entreprise qui met en œuvre un traitement de données à caractère personnel, automatisé en tout ou en partie ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

Les entreprises sont presque toutes concernées dans la mesure où l'entreprise traite des données personnelles de ses salariés dans le cadre de la gestion des ressources humaines ou de ses clients dans le cadre de la gestion des clients/prospects.

Le RGPD ne s'applique pas au traitement de données à caractère personnel effectué par une personne physique dans le cadre d'une activité strictement personnelle ou domestique.

En outre, certaines dispositions pourront ne pas s'appliquer à votre situation. Certaines dispositions du RGPD comportant des conditions et des exceptions, une analyse au cas par cas est ainsi nécessaire pour vérifier si telle ou telle obligation du RGPD s'applique à votre entreprise.

5. Existe-t-il un mode d'emploi pour se mettre en conformité ?

Le RGPD est un texte général qui fixe les règles relatives à la protection des données personnelles. Il n'existe pas de mode d'emploi pour se mettre en conformité. Une analyse de la situation de l'entreprise est nécessaire pour déterminer les actions qui devront être mises en œuvre par l'entreprise pour se mettre en conformité et le rester.

La mise en conformité nécessite en outre de recourir à des compétences de nature très différente : juridique, organisationnelle et technique et de travailler en transversalité (une grande partie des salariés sont amenés à traiter au quotidien des données personnelles et doivent être informés et sensibilisés aux processus et procédures internes de l'entreprise).

6. Que faut-il faire pour être en conformité ?

En fonction de l'entreprise, les actions à mener pourront être très différentes (cf. question n° 5).

Des documents de référence (outils, fiches PraTIC, textes officiels, etc.) sont mis à disposition des adhérents de Syntec Numérique pour leur permettre de prendre connaissance et comprendre les nouvelles règles applicables dès le 25 mai 2018. Ils sont accessibles dans la rubrique dédiée au RGPD sur le site de Syntec Numérique.

Un accompagnement pourra s'avérer utile. C'est pourquoi Syntec Numérique a référencé ses adhérents qui proposent des prestations d'accompagnement dédiées au RGPD. Elles sont classées dans quatre catégories :

1. Audit de conformité/Diagnostic/Plan de mise en conformité
2. Formation et sensibilisation
3. Délégué à la protection des données personnelles (DPD) externalisé
4. Solutions techniques (registre, effacement, sécurité, anonymisation, analyse d'impact, etc.)

7. Que va-t-il se passer le 25 mai 2018 ?

Le RGPD est entré en vigueur en 2016 et un délai de deux ans a été laissé aux entreprises pour se mettre en conformité avec les règles qu'il prévoit en matière de protection des données personnelles.

Le 25 mai 2018, toutes les entreprises devront donc être en conformité avec les règles prévues par le RGPD. Cela ne signifie pas que le 25 mai 2018, tout est terminé. En effet, ces règles s'appliquent à compter du 25 mai 2018.

8. Les formalités préalables effectuées avant le 25 mai 2018 exonèrent-elles l'entreprise du numérique de l'obligation de réaliser d'une analyse d'impact ?

La CNIL a indiqué, dans un article de février 2018, qu'elle n'exigera pas la « réalisation immédiate d'une analyse d'impact pour les traitements qui ont régulièrement fait l'objet d'une formalité préalable auprès de la CNIL avant le 25 mai 2018 (récépissé, autorisation, avis de la CNIL) ou qui ont été consignés au registre d'un correspondant informatique et libertés. De tels traitements ne seront donc pas soumis immédiatement à l'obligation d'analyse d'impact ».

La CNIL a précisé que les traitements en cours après le 25 mai 2018 et susceptibles de présenter un risque élevé devront faire l'objet d'une analyse d'impact « dans un délai raisonnable qui peut être estimé à 3 ans à compter du 25 mai 2018 ».

En revanche, l'analyse d'impact devra être réalisée, sans attendre l'issue de ce délai de trois ans, dans tous les autres cas où un traitement est susceptible de présenter un risque élevé :

- → pour les traitements antérieurs au 25 mai 2018 n'ayant pas fait l'objet de formalités préalables auprès de la CNIL ;
- → pour les traitements, antérieurs au 25 mai 2018 et régulièrement mis en œuvre, mais qui ont fait l'objet d'une modification substantielle depuis l'accomplissement de leur formalité préalable ;
- → pour tout nouveau traitement après le 25 mai 2018.

9. Les certifications/codes de conduite prévus par le RGPD sont-ils disponibles ?

Le RGPD prévoit des dispositions spécifiques sur les codes de conduite et la certification qui permettent aux responsables du traitement et aux sous-traitants de démontrer le respect de certaines de leurs obligations respectives.

Concernant la certification, les référentiels ne sont pas encore disponibles. La CNIL a ainsi indiqué, dans un article publié fin février 2018, que les travaux sur les référentiels de certification avaient débuté notamment concernant la formation et le délégué à la protection des données personnelles. Les référentiels seront élaborés après une phase de consultation publique, approuvés par la CNIL et publiés sur son site internet.

Concernant les codes de conduite, ils peuvent être élaborés par des associations ou organismes représentant des catégories de responsables du traitement ou de sous-traitants aux fins de préciser les modalités d'application du RGPD et seront soumis à l'approbation de l'autorité de contrôle nationale ou à la Commission européenne après avis du Comité européen de la protection des données si le code de conduite concerne des activités de traitement menées dans plusieurs Etats membres de l'Union européenne.

Outre l'avantage concurrentiel que pourra constituer l'application de codes de bonne conduite et/ou de certifications approuvés, l'autorité de contrôle pourra prendre en compte leur application pour décider s'il y a lieu d'imposer une amende administrative et du montant de celle-ci.

10. Quelles sont les sanctions ?

La CNIL peut adopter des mesures correctrices : avertissement, rappel à l'ordre, retrait des certifications, suspension des transferts de données dans un pays tiers à l'Union européenne ou à une organisation internationale, etc.

La CNIL peut également prononcer des amendes administratives : jusqu'à 20 000 000 d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent. A titre de comparaison, la CNIL peut actuellement prononcer des sanctions administratives pouvant s'élever à 3 millions d'euros.

Il convient également de ne pas négliger le risque judiciaire : un risque pénal avec des peines d'emprisonnement et d'amendes ainsi que le risque civil avec des dommages et intérêts.

Cette foire aux questions a été réalisée sur la base des textes législatifs et réglementaires en vigueur au moment de sa rédaction. Elle ne constitue nullement un conseil personnalisé et n'a pas pour vocation à se substituer aux conseils d'un avocat. Elle ne saurait à ce titre en aucun cas entrainer la responsabilité de Syntec Numérique ou de son représentant.

Contacts Syntec Numérique : Emilie Dumérain, déléguée juridique et Cloé Ahoulou, Juriste-Chargée de mission