Règlement général sur la protection des données (RGPD)

Le guide pratique Sage pour les entreprises

Table des matières

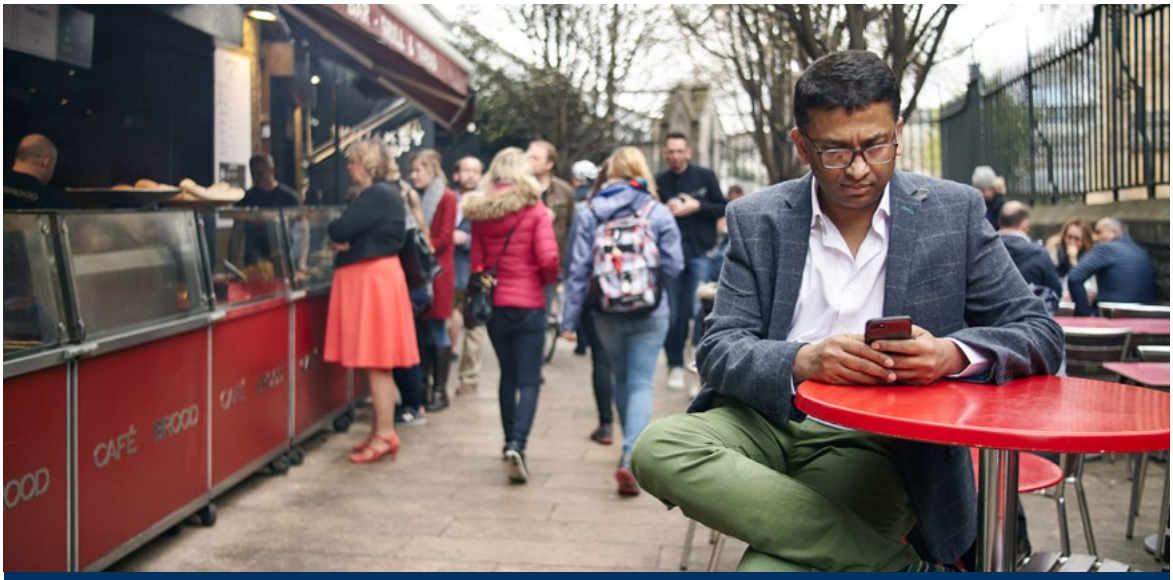
Introduction

Le Règlement général sur la Protection des données (RGPD) est le nouveau cadre légal qui prendra effet le 25 mai 2018 dans l'Union européenne (UE). Les réglementations européennes ont une incidence directe sur les États membres de l'UE, en ce sens que le RGPD primera sur toutes les lois nationales.

Le RGPD a pour objet la protection des données à caractère personnel, c'est-à-dire les données concernant les individus. Il s'agit de l'un des plus grands bouleversements de la réglementation encadrant le traitement des données à caractère personnel. Le RGPD concerne non seulement les entreprises, mais potentiellement toute personne, entreprise, autorité ou administration publique, ou toute autre organisation traitant les données à caractère personnel de résidents de l'UE. Sont inclus notamment dans cette liste les fournisseurs ou tout autre tiers auxquels une entreprise peut faire appel pour gérer les données à caractère personnel.

Le champ d'application du texte est étonnamment vaste, puisqu'il englobe tous les États membres de l'Union européenne, ainsi que le Royaume-Uni post Brexit en 2019, car le RGPD sera intégré à la législation britannique. Contrairement à la Directive 95/46 de l'UE sur les règles de protection des données à caractère personnel, le RGPD concernera également les sociétés basées en dehors de l'UE qui proposent des biens ou des services aux résidents de l'UE, ou qui étudient leur comportement au sein de l'UE. Par exemple, les sociétés d'hébergement de sites Internet situées aux États-Unis et hébergeant des sites consultables par des personnes vivant dans l'UE sont directement impactées.

Dans le monde entier, de nombreuses entreprises vont être confrontées aux implications très importantes de ce texte pour chacune de leurs fonctions. Certaines entreprises auront besoin d'embaucher ou de désigner un Délégué à la protection des données (Data Protection Officer – DPO). La plupart d'entre elles seront obligées de mettre en œuvre des mesures et des garde-fous supplémentaires. Faire mener un audit par un professionnel qualifié est vivement recommandé. Compte tenu également des risques de sanctions financières pouvant atteindre 4 % du chiffre d'affaires mondial annuel ou 20 millions d'euros (le montant le plus élevé étant retenu), une bonne compréhension du RGPD est indispensable.



Ce document se veut un guide concis et simplifié pour les entreprises. Des informations complémentaires sont disponibles auprès de l'autorité de contrôle, soit la CNIL en France, et sur son site Internet « Se préparer au Règlement général sur la protection des données ». Veuillez prendre connaissance de la Limitation de responsabilité Sage présentée à la fin de ce guide.

Infographie :

Comprendre le RGPD en un clin d'oeil

Règlement général sur la Protection des données (RGPD)

Consentement

Doit être confirmé par une déclaration ou un acte positif clair. Le consentement ne peut être tacite et les cases pré-cochées sur les sites web sont interdites.

Droits des personnes

Développe considérablement les droits des personnes et le nombre d'informations à leur communiquer au sujet du traitement.

Délégué à la protection des données

Peut être obligatoire dans certains cas. A une connaissance approfondie de la loi sur la protection des données. Salarié ou employé sous contrat de prestation de services.

Sanctions

Jusqu'à 4 % du CA annuel mondial ou 20 millions d'euros (le montant le plus élevé étant retenu). Une amende est possible même sans perte de données.

Respect de la vie privée tout au long du processus

Le traitement intègre la vie privée à chaque étape et n'utilise que les données strictement nécessaires à la finalité indiquée.

Portabilité des données

Les personnes peuvent récupérer, stocker ou transmettre leurs données, même chez un concurrent.

Champ d'application élargi

S'applique à votre entreprise et à celles traitant les données pour vous, même en dehors de l'UE.

Notification obligatoire des failles de sécurité

Les responsables de traitement des données en France doivent prévenir l'Autorité de contrôle compétente 72 heures maximum après en avoir pris connaissance. Doivent avertir la personne concernée en cas de risque élevé pour les droits et libertés de la personne concernée.

Principales dispositions

Le RGPD fixe les obligations minimales à respecter pour le traitement de toutes les données à caractère personnel. On peut définir les données à caractère personnel comme l'ensemble des informations permettant l'identification d'un individu ou se rapportant principalement à cet individu (notamment des caractéristiques comme l'apparence physique ou même les données biométriques).

La plupart des entreprises commencent à recueillir des données personnelles dès le premier contact avec un individu. Dans certains cas, elles n'ont même pas conscience de le faire. Le simple fait d'utiliser des cookies persistants pour identifier les visiteurs de votre site Internet est déjà considéré comme un recueil de données à caractère personnel. Tout comme l'historique détaillé d'une personne dans une base de données utilisée pour la gestion de la relation clients (CRM). Même si les données à caractère personnel sont recueillies ou traitées uniquement au profit de l'individu en question, elles sont encore du ressort du RGPD.

Comme pour la Directive européenne 95/46, le RGPD reprend trois groupes de règles fondamentales s'appliquant aux données à caractère personnel : les principes de protection des données, la licéité du traitement et les restrictions sur les transferts hors UE. Ces règles devraient déjà être connues de la plupart des entreprises et de nombreuses personnes. Ces trois groupes de règles sont abordés plus loin de façon plus détaillée ; leur lecture s'impose même s'il ne s'agit que de vous rafraîchir la mémoire.

Le RGPD intègre également plusieurs nouvelles obligations de taille.

Le RGPD en résumé

Voici les principaux domaines couverts par le RGPD, qui reprend en partie la Directive européenne 95/46 sur la protection des données à caractère personnel.

Droits des personnes— et comment les faire connaître

Jusqu'à présent, la législation européenne sur la protection des données (Directive 95/46) conférait aux particuliers certains droits sur leurs données à caractère personnel et énonçait les informations qui devaient leur être communiquées par les responsables de traitement, notamment les informations concernant leur utilisation de ces données. Ces informations prenaient souvent la forme de déclarations ou d'avertissements relatifs au respect de la vie privée intégrés à un site Internet.

Ces dispositions sont considérablement élargies par le RGDP qui octroie des droits supplémentaires aux personnes concernées, qui doivent être informées. En particulier, les personnes doivent être informées qu'elles disposent des droits inclus dans la liste non exhaustive suivante, notamment les droits :

1. de se plaindre auprès de l'autorité de contrôle compétente, telle que la CNIL en France
2. de retirer leur consentement au traitement de leurs données à caractère personnel (voir ci-dessous)
3. d'accéder à leurs données personnelles et de les faire rectifier ou effacer (le « droit à l'oubli ») par l'entreprise et tous les tiers qui ont pu y avoir accès
4. d'être informées de l'existence de tout traitement automatisé des données à caractère personnel (notamment le profilage)
5. de s'opposer à certaines formes de traitement, par ex. le marketing direct ou des décisions fondées exclusivement sur un traitement automatisé
6. de connaître la durée de conservation de leurs données à caractère personnel
7. d'être destinataires des informations relatives à la nomination d'un Délégué à la protection des données (voir ci-dessous).

De plus, les personnes concernées ont le droit de demander à des organisations à but non lucratif de faire valoir leurs droits et d'intenter des actions en leur nom, à l'instar des actions de groupe pratiquées aux États-Unis.

Consentement

Alors que la législation européenne sur la protection des données a toujours exigé que le consentement des personnes concernées au recueil de leurs données soit libre, spécifique et donné en connaissance de cause, le RGPD demande dorénavant qu'il soit confirmé par une déclaration ou par un autre acte positif clair. En d'autres termes, les cases pré-cochées sur les sites Internet ou le silence/l'inactivité de la personne concernée après lecture d'une déclaration sur le respect de la vie privée ne peuvent valoir consentement.

De plus, le consentement ne peut pas être polyvalent, c'est-à-dire qu'une entreprise ne peut pas considérer que le consentement reçu d'une personne à un certain moment de leur relation commerciale vaut consentement pour d'autres types de traitement de données à caractère personnel. Chaque type de traitement de données à caractère personnel doit faire l'objet d'un consentement spécifique.

Enfin, les personnes concernées doivent non seulement être informées qu'elles ont le droit de retirer leur consentement à tout moment, mais elles doivent pouvoir retirer ce consentement aussi facilement qu'elles l'ont donné.

Il est indispensable de passer en revue les consentements préalablement donnés par des individus pour s'assurer de leur conformité aux dispositions du RGPD. En cas de conflits ou d'ambiguïtés, les entreprises ont le choix entre trouver une nouvelle justification légale au traitement des données (ce dernier est par exemple indispensable à l'exécution d'un contrat) et recueillir un nouveau consentement, ou arrêter complètement le traitement de ces données à caractère personnel.

Droit de déplacer ou de transférer les données à caractère personnel (portabilité des données)

Les personnes concernées ont désormais le droit de recevoir, stocker et de transférer leurs données à caractère personnel d'un prestataire vers un autre, même s'il s'agit d'un concurrent. Ainsi, un utilisateur qui a créé une playlist avec un service de musique pourra la faire chez un autre prestataire s'il décide d'en changer. C'est pourquoi les données à caractère personnel doivent être conservées dans un format structuré, couramment utilisé et lisible par machine, pour pouvoir être facilement utilisées et communiquées.

L'obligation d'assurer la portabilité et de faciliter l'utilisation des données par d'autres prestataires entraînera probablement des modifications au niveau IT et par conséquent des coûts supplémentaires.

Un champ d'application très élargi

Avec le RGPD, la responsabilité des failles de sécurité n'incombe pas seulement au responsable de traitement qui recueille les données à caractère personnel, mais également à tout sous-traitant chargé du traitement des données par ce responsable de traitement, que le sous-traitant soit une autre société, une organisation ou une personne physique. Cette responsabilité ne signifie pas qu'une entreprise peut se contenter de déléguer le traitement des données à un tiers et de fermer les yeux. Le responsable de traitement doit veiller à ce que le fournisseur tiers respecte lui-aussi le RGDP.

De plus, le périmètre géographique concerné est potentiellement élargi au-delà de l'UE pour les entreprises — ou pour les tiers traitant des données à caractère personnel pour le compte de ces entreprises— qui proposent des biens ou des services à des résidents européens, ou qui étudient leur comportement. Il convient de remarquer que ces dispositions s'appliquent, que les biens ou les services proposés soient payants ou non ; par conséquent les organisations caritatives et les ONG sont également concernées par le RGPD.

Comme l'UE est partenaire commercial de la plupart des pays, l'élargissement du champ d'application du RGPD aura des conséquences pour un grand nombre d'entreprises du monde entier, qui devront afficher leur conformité pour travailler dans les États membres de l'UE, directement ou en tant que tiers pour d'autres acteurs.

Faire la preuve de la conformité

Être conforme au RGPD n'est plus une condition suffisante. Toute entreprise devra pouvoir prouver qu'elle répond à l'exigence de « responsabilité » prévue dans le RGPD, ce qui lui demandera d'être conforme à un certain nombre d'obligations de tenue de registre assez coûteuses. Plus précisément, un registre devra être tenu qui répertoriera les activités de traitement*, les demandes d'accès aux données, les failles de sécurité, les modalités de recueil du consentement, et des études d'impact sur la vie privée (voir ci-dessous).

Cette obligation concerne également les tiers chargés du traitement des données à caractère personnel pour le compte d'une autre entreprise, même si les exigences ne sont pas aussi détaillées.

** S'applique aux entreprises de plus de 250 salariés, ou aux entreprises avec des effectifs inférieurs dans lesquelles le traitement des données est susceptible de créer un risque pour les droits et les libertés des individus, n'est pas occasionnel ou concerne des catégories de données particulières, par exemple des informations sur la santé, la religion ou l'orientation sexuelle.*

Respect de la vie privée tout au long du processus

Des mesures techniques et organisationnelles doivent être mises en œuvre pendant toute la durée de vie des données à caractère personnel, de la conception à la fin des opérations de traitement, pour répondre aux attentes des individus concernés en matière de respect de la vie privée. Cette disposition du texte est intitulée « Respect de la vie privée dès la conception », ce qui signifie que tous les aspects liés à la vie privée doivent être pris en compte et intégrés au traitement dès sa conception.

De plus, le traitement devra exploiter uniquement les données à caractère personnel strictement nécessaires à la finalité de ce traitement, répondant au principe de minimisation des données ou de « Respect de la vie privée par défaut ».

En pratique, l'application des principes de respect de la vie privée, dès la conception ou par défaut, nécessitera de proposer en permanence des formations, de recueillir le moins de données possible, de limiter l'accès aux données à caractère personnel aux utilisateurs en ayant vraiment besoin, et à mettre en oeuvre des mesures de sécurité techniques et organisationnelles pertinentes, telles que la pseudonymisation et le chiffrement des données.

Notification obligatoire des failles de sécurité

En cas de faille de sécurité, les entreprises recueillant des données à caractère personnel doivent prévenir l'autorité de contrôle - comme la CNIL en France - 72 heures au plus tard après en avoir été informées. Les prestataires tiers traitant les données à caractère personnel pour le compte de ces entreprises doivent avertir celles-ci dans les plus brefs délais.

Si cette faille présente un risque élevé pour les personnes concernées, les entreprises doivent également les prévenir dans les plus brefs délais.

Délégué à la protection des données (DPO)

En vertu du RGPD, les entreprises traitant des données à caractère personnel, ou leurs sous-traitants, doivent désigner un Délégué à la protection des données (DPO) : (i) si elles appartiennent au service public ; (ii) si leur activité principale les amène à réaliser un suivi des personnes à grande échelle ; ou si leur activité principale les amène à traiter à grande échelle des catégories particulières de données, notamment celles relatives à des condamnations ou à des infractions pénales. Le DPO doit avoir une connaissance approfondie de la législation sur la protection des données. Il ne s'agit pas obligatoirement d'un salarié de l'entreprise et il est parfaitement envisageable de l'employer sur la base d'un contrat de prestation de services. Les coordonnées du DPO doivent être communiquées à l'autorité de contrôle, soit la CNIL en France.

Sanctions

Les sanctions pour non-respect du RGPD sont lourdes et peuvent atteindre 4 % du chiffre d'affaires mondial annuel ou 20 millions d'euros (le montant le plus élevé étant retenu). Vous pouvez encourir une amende même si aucune donnée n'est perdue. Il convient de noter qu'il n'existe aucune exemption ou exception pour les petites entreprises. Par ailleurs, toute personne a le droit d'intenter une action de groupe en demandant l'ouverture d'une enquête réglementaire officielle si elle considère qu'une entreprise est en infraction avec le RGPD

A propos du Brexit

Suite aux élections législatives britanniques de 2017, le gouvernement conservateur entame un nouveau mandat de cinq ans. Au cours de ce mandat, en 2019 précisément, le Royaume-Uni quittera l'UE. Jusqu'à cette date, le RGPD s'appliquera au Royaume-Uni, comme à tous les États membres de l'UE. Cependant, l'annonce d'une nouvelle législation à la suite des élections était accompagnée d'une déclaration selon laquelle les nouvelles lois sur la protection des données :

« ... mettront en œuvre le Règlement général pour la Protection des données et la nouvelle Directive concernant le traitement des données pour l'application des lois, en remplissant nos obligations tant que nous serons un État membre de l'UE et en plaçant le Royaume-Uni dans la meilleure configuration possible pour conserver notre capacité à partager des données, avec les autres États membres de l'UE et au niveau international, après notre départ de l'UE. »

(Source : Discours de la Reine, juin 2017)

On peut donc imaginer sans en être certain qu'après le Brexit, le Royaume-Uni soit considéré par la Commission européenne comme un pays offrant une « protection adéquate » et ne soit pas confronté à des problèmes tels que les interdictions de transferts mises en œuvre pour la protection des données.

La nouvelle législation britannique remplace le Data Protection Act 1998, qui s'appuyait sur la Directive UE 95/46.

Principes fondamentaux du RGPD

En plus des nouvelles obligations présentées plus haut, et comme pour la Directive européenne 95/46, le RGPD reprend trois groupes de règles fondamentales s'appliquant aux données à caractère personnel. Il est possible de les résumer comme suit :

- ***Principes de protection des données :*** Les données à caractère personnel doivent être traitées de manière loyale, licite et transparente pour la personne concernée. Les données ne doivent être recueillies que pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Les données recueillies doivent être adéquates, pertinentes et limitées à ce qui est nécessaire. Elles doivent être exactes et actualisées régulièrement, et toutes les mesures raisonnables doivent être prises pour que les données inexactes soient rectifiées ou effacées dans les plus brefs délais. Les données doivent être conservées de manière à ne pas permettre l'identification de la personne concernée au-delà du temps nécessaire, et traitées de façon à garantir une protection appropriée – notamment contre la perte, la destruction, ou les dommages, et contre les accès non autorisés ou illégaux.
- ***Licéité du traitement :*** Le traitement des données à caractère personnel est licite uniquement si au moins l'une des conditions suivantes est remplie : la personne concernée a consenti au traitement pour une ou plusieurs finalités spécifiques ; le traitement est nécessaire à l'exécution d'un contrat dont la personne concernée est ou sera bientôt partie prenante ; il existe une obligation légale (par ex. la transmission des dossiers fiscaux par une entreprise) ; il existe une mission d'intérêt public ou qui est effectuée dans l'intérêt de l'autorité publique ; le traitement est nécessaire aux fins des intérêts légitimes du responsable de traitement (ou d'un tiers), à moins que ne prévalent les intérêts, les droits fondamentaux ou les libertés de la personne concernée.
- ***Transferts en dehors de l'UE :*** Le RGPD prolonge l'interdiction générale de transférer des données à caractère personnel en dehors de l'Espace économique européen vers un pays n'offrant pas un niveau de protection adéquat. Au moment de la rédaction de ce document, les pays reconnus par la Commission européenne comme offrant une protection « adéquate » sont : les entreprises américaines qui ont certifié respecter l'accord Privacy Shield Union européenne-États-Unis (remarque : ce n'est pas pour autant que les États-Unis sont reconnus comme un pays offrant une protection adéquate), Andorre, Argentine, Canada (limité au PIPEDA), îles Féroé, Guernesey, Israël, île de Man, Jersey, Nouvelle-Zélande, Suisse et Uruguay. En l'absence de décision d'adéquation, les transferts ne peuvent avoir lieu que dans des circonstances limitées, notamment, sur la base du consentement, l'utilisation des clauses contractuelles types publiées par la Commission européenne ou, dans le cas des transferts inter-sociétés, l'utilisation des Règles d'entreprise contraignantes (BCR, Binding Corporate Rules).

Les mesures à prendre dès aujourd'hui

- Consultez la rubrique Règlement européen du site Internet de la CNIL pour en savoir plus, vous y trouverez des conseils pratiques et des informations d'ordre général. En particulier, consultez les pages « Se préparer au Règlement général sur la protection des données ».
- Passez en revue vos systèmes de recueil et de traitement des données à caractère personnel pour vérifier leur conformité au RGPD. Vous pouvez envisager, parmi d'autres mesures, de conduire un audit RGPD sur les plans juridique et technologique.
- Parlez du RGPD à vos salariés et à vos partenaires, et planifiez des formations pour les y préparer. Rappelez-vous qu'en vertu du RGPD, vous êtes responsable des tiers qui traitent les données à caractère personnel pour votre compte.
- Demandez un avis juridique pour bien comprendre les implications du RGPD sur votre activité.

Pour en savoir plus, veuillez consulter : sage.com/RGPD

Limitation de responsabilité Sage

Les informations communiquées dans ce guide sont fournies à titre indicatif uniquement. Elles ne visent pas à constituer un conseil juridique et ne doivent pas être interprétées comme tel. Nous tenons à souligner que, pour les clients qui ne sont pas certains des implications du RGPD pour leurs activités, rien ne peut remplacer la conduite de leur propre enquête approfondie ou l'obtention de conseils juridiques spécifiques à leur situation.

Bien que nous ayons tout mis en œuvre pour faire en sorte que les informations apportées sur ce site Internet soient exactes et actualisées, Sage ne fait aucune promesse quant à leur exhaustivité ou à leur exactitude, et les informations sont fournies « telles quelles » sans aucune garantie, expresse ou implicite. Sage ne pourra être tenu responsable d'éventuelles erreurs ou omissions et sa responsabilité ne saurait être engagée pour tout dommage (y compris, mais sans s'y limiter, les pertes commerciales ou les pertes de bénéfices), contractuel, délictuel ou autre, résultant de l'utilisation de ces informations ou de la confiance accordée à ces informations, ou de toute mesure ou décision prise à la suite de l'utilisation de ces informations.