ANNEXE 2 : INFORMATIONS CONCERNANT LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

Règlement général sur la protection des données

Le RGPD (GDPR, en anglais) porte sur la gestion et la protection des données personnelles des citoyens européens. Toute organisation doit, dès mai 2018 pouvoir renseigner toute personne sur les données que vous collectez sur elle, l'utilisation que vous en faites et la façon dont vous les protégez (et ce, que vous disposiez de votre propre centre de données ou que vous les gériez depuis un cloud situé hors UE).

Le RGPD en bref :

- Protection des données personnelles du citoyen européen
- Mesures contre les hackers et fuites de données
- En vigueur dès le 25 mai 2018
- Procédure pour la collecte et l'enregistrement de données personnelles
- Demande de consentement nécessaire pour la collecte et l'utilisation de données
- 'Droit à l'oubli' pour chaque individu
- Mesures de sécurité plus strictes requises
- Obligation de signaler toute fuite de données endéans les 72 heures
- Les autorités nationales peuvent appliquer des amendes
- Dans les grandes organisations, un Délégué à la protection des données (DPD) doit être désigné

Principes de base de la protection des données

La protection des données s'articule autour de principes de base. Ces principes sont déjà repris dans les textes de loi actuellement en vigueur, mais se voient renforcés par le RGPD. Chaque responsable du traitement des données devra respecter ces principes.

Licéité, loyauté et transparence

Ce principe porte sur l'obligation de traiter les données en toute licéité, loyauté et transparence vis-à-vis de la personne concernée.

L'article 30 explicite ce qui est entendu par transparence : il doit être parfaitement clair pour les individus que leurs données sont collectées, utilisées, consultées ou traitées de toute autre manière. Le principe de transparence exige que toute information ou communication portant sur le traitement des données doit être accessible et compréhensible.

Le langage utilisé doit donc être clair et simple. Le responsable du traitement des données doit être clairement identifié, tout comme la finalité du traitement. Les informations complémentaires qui peuvent être demandées doivent être précisées, afin de garantir un traitement loyal et transparent. Les individus doivent être informés des risques, des règles, des garanties et des droits que comportent le traitement, ainsi que de la façon dont ils peuvent faire valoir leurs droits.

Ce principe est lié à l'article 6 du Règlement, qui énumère les raisons justifiant un traitement des données. Cet article détermine les conditions permettant de juger si un traitement est licite ou non. Retrouvez plus d'informations sur cet article 6 sous le point consacré à la licéité du traitement.

Exactitude

Les données doivent être exactes et à jour. Tous les efforts raisonnables doivent être faits pour supprimer ou corriger sans délai les données inexactes ou incomplètes, en fonction de l'objectif de collecte et de traitement.

Intégrité et confidentialité

Le RGPD exige une protection appropriée des données traitées, moyennant des mesures techniques et organisationnelles adaptées.

Ceci implique une protection contre le traitement non autorisé ou illicite, la perte, la destruction ou le déficit en qualité des données.

L'article 39 stipule que le traitement des données doit se faire de manière à garantir la protection et la confidentialité des données. Tout risque d'accès illicite aux données et de communication illicite des données doit être atténué.

Qu'est-ce qui change ?

L'obligation de veiller à des procédures de traitement sûres existait déjà depuis la Directive européenne 95/46/CE, mais n'était pas reprise en tant que principe de base de la protection des données. Le concept même de la protection des données est modifié et prend un caractère plus technique.

Limitation des finalités

Le principe de finalité détermine que la collecte de données personnelles doit répondre à des finalités déterminées, explicites et légitimes. Il est interdit de traiter ultérieurement ces données d'une manière incompatible avec ces finalités.

L'article 89.1 du RGPD prévoit que le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques peuvent constituer des dérogations à l'incompatibilité.

Le principe de finalité spécifique existe déjà dans les lois actuellement en vigueur.

Qu'est-ce qui change ?

Dans l'article 6.4, le RGPD autorise le traitement de données personnelles à d'autres fins que les finalités initiales de collecte des données, mais uniquement si ce traitement est compatible avec les finalités initiales. Dans ce cas, aucun autre fondement juridique ne sera requis que le fondement ayant autorisé la collecte des données personnelles.

Afin de vérifier si la finalité d'un traitement est compatible avec la finalité initiale, le responsable du traitement, après s'être assuré de répondre aux prescriptions en matière de licéité lors du traitement initial des données, doit effectuer une vérification de la compatibilité.

Le responsable du traitement, afin de déterminer si le traitement à une autre fin est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, tient compte, entre autres :

- de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé ;
- du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;
- de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, en vertu de l'article 9, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 10 ;
- des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;
- de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

Toutefois, lorsque le traitement à une fin autre que celle pour laquelle les données ont été collectées est fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre, le responsable du traitement pourra procéder au traitement, qu'il soit compatible ou non avec les finalités initiales.

Minimisation des données

D'après le principe de minimisation du traitement des données, les données traités doivent être pertinentes, adéquates et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

L'objectif est que le responsable du traitement ne traite que les données nécessaires aux finalités spécifiques. Le mot d'ordre est donc de traiter uniquement le strict minimum.

L'article 39 clarifie la mission du délégué à la protection des données : celui-ci doit veiller à ce que la durée de conservation des données soit limitée au strict minimum. Il doit également s'assurer que les données personnelles ne soient traitées que si la finalité du traitement ne peut être atteinte d'aucune autre façon.

Ce principe existait déjà dans la Directive européenne 95/46/CE, bien que sous un autre nom.

Limitation de la conservation

Les données ne peuvent être conservées que pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. La forme de conservation doit garantir la possibilité d'identifier les personnes concernées.

Les données ne peuvent être conservées pour une donnée plus longue qu'à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques. Ce traitement doit être compatible avec l'article 89 du RGPD.

Afin de garantir que les données ne soient pas conservées plus longtemps que nécessaire, des délais doivent notamment être fixés pour leur effacement. Enfin, des mécanismes doivent être mis en place afin de pouvoir vérifier l'inaccessibilité des données à l'issue de ce délai.