

Règlement général de l'UE sur la protection des données

Etat : 01.07.2018

Généralités

Le règlement général de l'UE sur la protection des données (ci-après « RGPD-UE ») est en vigueur depuis le 25 mai 2018. Il garantit un niveau de protection des données plus élevé que les dispositions de droit suisse, et accorde des droits plus étendus aux personnes concernées (droits d'information, de rectification, de consentement au partage des données, etc.). Le RGPD-UE concerne, à certaines conditions, également les Etats non-membres de l'UE. La présente précise ci-après dans quelle mesure le RGPD-UE s'applique aux membres du SVIT. Indépendamment de la question de savoir si le RGPD-UE s'applique ou non, la présente indique également quelles sont les mesures à prendre afin d'assurer le respect de la réglementation européenne. L'accent sera mis en particulier sur l'exploitation et la maintenance des sites internet des membres du SVIT.

Cadre légal/Champ d'application du RGPD-UE

Conformément au « principe du lieu où se tient le marché », le RGPD-UE s'applique non seulement dans l'UE, mais peut également déployer ses effets dans des pays situés hors de l'UE. Le champ d'application territorial (extraterritorial) du RGPD-UE est défini à l'art. 3 al. 2 RGPD-UE. La teneur de cet article est la suivante :

Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:

- a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou*
- b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.*

Avant d'interpréter les dispositions du règlement, il convient de brièvement définir les notions utilisées dans celui-ci.

Définitions

Données à caractère personnel (art. 4 al. 1 RGPD-UE): les « données à caractère personnel » sont toutes les informations se rapportant à une personne physique identifiée ou identifiable (ci-après « personne concernée ») ; est réputée 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. A titre d'exemple, les données ci-après sont des données à caractère personnel : nom, adresse, date de naissance, données bancaires.

Traitement (de données) (art. 4 al. 2 RGPD-UE) : le « traitement » consiste en toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués 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.

Responsable du traitement (art. 4 al. 7 RGPD-UE) : le « responsable du traitement » est la personne physique ou morale, l'autorité publique, le service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Sous-traitant (art. 4 al. 8 RGPD-UE) : le « sous-traitant » est 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.

Champ d'application selon l'art. 3 al. 2 let. a RGPD-UE

La question de savoir si les membres du SVIT offrent des « biens ou services dans l'Union » est déterminante pour le champ d'application selon l'art. 3 al. 2 let. a RGPD-UE. Le RGPD-UE ne définit pas précisément la notion d'offre de biens et services. La question se pose donc de savoir si, pour que le RGPD-UE trouve à s'appliquer, les biens et services offerts doivent effectivement être exportés dans l'UE (p.ex. un CH-*Onlineshop* qui vend, respectivement expédie, de la marchandise en Allemagne), ou s'il suffit que l'offre ne puisse être « acceptée » que par des personnes résidant dans l'UE (p.ex. : un couple résidant en Allemagne achète sur un site internet une maison de vacances offerte par un membre du SVIT au bord du Lac des Quatre-Cantons)

A teneur du libellé du règlement, l'unique question est de savoir si les personnes résidant dans l'UE se voient offrir des biens ou des services. Le lieu où la prestation est effectivement exécutée (UE ou Suisse) ne semble pas déterminant. En vertu du considérant 23 RGPD-UE, l'accessibilité de l'offre dans un Etat membre de l'UE (p.ex. par le biais de sites internet) n'est toutefois pas suffisante dans ce contexte. Il convient en particulier de déterminer si les biens et services sont offerts dans une langue et/ou une monnaie d'usage courant dans un ou plusieurs pays de l'UE.

La question du champ d'application selon l'art. 3 al. 2 RGPD-UE ne peut pas être tranchée de manière définitive. Toutefois, le libellé de la disposition et certaines autres indications (p.ex. toute offre sur le site internet d'un membre du SVIT dans une langue/monnaie d'usage courant dans un Etat membre de l'UE) pourraient toutefois plaider en faveur de l'applicabilité du RGPD-UE.

Champ d'application selon l'art. 3 al. 2 let. b RGPD-UE

Le RGPD-UE est également applicable lorsque les activités de traitement sont liées au suivi du comportement des citoyens résidant dans l'UE, en particulier du comportement des utilisateurs d'internet. A teneur du considérant 24 RGPD-UE, afin d'établir si une activité de traitement peut être considérée comme un suivi du comportement, il y a lieu d'établir si la personne concernée est suivie sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel

qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit.

Un suivi au sens de l'art. 3 al. 2 let. b RGPD-UE pourrait exister lorsque des *cookies* (y compris Google Analytics), *social media plug-ins* ou autres *internet-tags* sont utilisés sur un site internet. Il s'agit d'applications qui permettent à un site internet de reconnaître l'ordinateur de l'utilisateur et de sauvegarder des informations relatives à chaque visite sur le site internet (recherches, informations sur les sites internet visités au préalable, préférences/réglages sur le site internet, etc.). A cet effet, il convient de faire la distinction entre, d'une part, les *cookies* de fonctionnalité et de performance et, d'autre part, les *cookies* de suivi et de ciblage. Ces premiers ne sont pas pertinents en termes de législation sur la protection des données et n'entraînent pas l'applicabilité du RGPD-UE (pas de suivi, respectivement de profilage). L'utilisation de *cookies* de suivi et de ciblage peut toutefois conduire à une applicabilité des normes européennes, dès lors que lesdits *cookies* peuvent être utilisés pour obtenir des informations relatives à l'historique de recherche de la personne concernée, informations pouvant ensuite être utilisées à des fins publicitaires.

Sur le site internet du SVIT Suisse, les visiteurs seront rendus attentifs à l'utilisation de *cookies* et de *social media plug-ins* (Facebook). Compte tenu de la large diffusion de ces applications, il y a lieu de considérer que de nombreux membres du SVIT utilisent également de tels programmes sur leurs sites internet. Il pourrait en résulter une applicabilité de principe du RGPD-UE dans le cadre de l'exploitation des sites internet des membres.

Recommandations

En partant du principe que le RGPD-UE s'applique aux parties, des mesures (à prendre immédiatement) sont présentées ci-après, à titre préventif, pour garantir le respect des dispositions du RGPD-UE en matière de protection des données.

Déclaration de confidentialité

Tous les sites internet des membres du SVIT devraient contenir une déclaration de confidentialité évoquant en particulier les thèmes suivants (un modèle de déclaration de confidentialité pour les sociétés immobilières est à disposition des membres au secrétariat de l'organisme membre) :

- Indication relative au traitement des données (avec mention du type de données traitées et but du traitement des données) ;
- Acceptation du consentement (tacite) au traitement des données dans le cas d'une communication volontaire de données personnelles ;
- Informations sur la sauvegarde, l'accès et la transmission des données ;
- Informations sur les *newsletter-marketing*, de même que sur l'utilisation de *cookies*, *social media plug-ins* et autre *internet-tags* ;
- Informations sur les droits des personnes concernées et coordonnées de la personne responsable du traitement.

Jusqu'à nouvel ordre, à chaque visite du site internet, une fenêtre faisant expressément référence à la déclaration de confidentialité et contenant un lien vers celle-ci devrait apparaître.

Indication relative à l'utilisation de *cookies* (*opt-in*)

La déclaration de confidentialité susmentionnée devrait également indiquer l'utilisation de *cookies*, *social media plug-ins* et autres *internet-tags*. Cette indication peut être formulée de la manière suivante : « Ce site internet utilise des *cookies*, *social media plug-ins* et autres *internet-tags*, afin de vous offrir une meilleure expérience d'utilisation. Par l'utilisation de ce site internet, vous acceptez l'utilisation de *cookies*, *social media plug-ins* et autres *internet-tags* ».

L'indication relative à l'utilisation de *cookies* peut également contenir une clause dite d'*opt-in*, à savoir une exigence de consentement explicite (« J'accepte » ou « Je refuse »)¹. Un refus signifierait que le site internet ne peut plus être utilisé par l'utilisateur concerné.

Newsletter-Marketing

L'envoi de newsletters reste autorisé sous le RGPD-UE. Dorénavant, certaines conditions doivent toutefois être remplies, de sorte que le traitement des données intervenant en lien avec lesdites newsletters respecte les nouvelles normes.

D'une part, le consentement actif de la personne concernée doit être obtenu, ce qui signifie que le consentement doit en principe figurer dans l'inscription (p.ex. par l'insertion d'une adresse e-mail)². D'autre part, une divulgation complète, transparente et compréhensible de la manière dont les données seront traitées est requise. Cette information peut être obtenue au moyen d'une déclaration de confidentialité. Enfin, les personnes concernées devraient pouvoir se désabonner à tout moment de la *newsletter* (fonction de désabonnement à la fin de chaque *newsletter*).

Conclusion

Bien que la question de l'applicabilité du RGPD-UE n'ait pas pu être définitivement clarifiée, il est recommandé à ce stade de se conformer aux nouvelles normes européennes. Dans le cadre de la mise en œuvre autonome, les dispositions relatives à la protection des données en vigueur en Suisse seront bientôt adaptées à celles de l'UE (révision de la LPD). La mise en œuvre de la recommandation devrait suffire à éviter toute sanction, compte tenu de l'incertitude juridique actuelle que l'entrée en vigueur du RGPD-UE a entraînée. Dans ce contexte, il convient également de noter que toute une série de mesures (moins sévères) (par ex. avertissements, annonces publiques) sont généralement prises avant que des sanctions ne soient infligées en vertu du RGPD-UE (en particulier des amendes). Néanmoins, les recommandations formulées dans la présente doivent être comprises comme des mesures devant être prises immédiatement.

Exclusion de responsabilité

Le SVIT Suisse précise que les présentes recommandations sont basées sur l'évaluation légale effectuée par l'association et sont faites sans garantie ni responsabilité aucune.

¹ Cette clause d'*opt-in* n'est pour l'instant pas encore exigé par la loi. Il existe toutefois d'ores et déjà une directive de l'UE relative aux *cookies*, laquelle vise à instaurer une obligation d'*opt-in*.

² Un double *opt-in*, en vertu duquel l'abonnement à la newsletter doit dans une seconde étape, après l'inscription, être expressément confirmé (p.ex. par e-mail), n'est pas requis pour le moment. Toutefois, le règlement de l'UE sur la protection de la vie privée dans le secteur des communications électroniques, qui devrait entrer en vigueur en 2019, prévoit une telle approche.