Les principales informations sur le nouveau droit de l'UE sur la protection des données

Le 25 mai 2018 entrera en vigueur le règlement de l'Union européenne sur la protection des données, abrégé «RGPD». Des entreprises suisses y seront également soumises. ch-direct résume les principales questions que se posent les entreprises de transport suisses et y répond.

Qu'est-ce que le RGPD?

Le RGPD forme le nouveau droit de l'UE sur la protection des données, qui s'appliquera directement dans tous les États-membres à partir du 25 mai 2018. Son champ d'application peut toutefois s'étendre à des entreprises situées en dehors de l'UE, mais qui traitent des données personnelles. Le RGPD vise à donner aux citoyens européens plus de contrôle sur leurs données personnelles, à responsabiliser davantage les entreprises tout en augmentant leurs charges déclaratives et à renforcer le rôle des autorités de protection des données.

Mon entreprise est-elle concernée par le nouveau RGPD?

Le champ d'application du RGPD est très large. Trois situations principales conduisent à une application du RGPD aux entreprises suisses traitant des données personnelles:

1. L'entreprise possède une filiale dans l'UE.
2. L'entreprise offre des biens et des services de façon ciblée à des personnes domiciliées dans l'UE. Elle s'y adresse manifestement et intentionnellement.
3. L'entreprise mène des «suivis du comportement» de personnes de l'UE.

Qu'entend le droit par «suivi du comportement»?

Le suivi du comportement renvoie principalement au *webtracking*. Quiconque utilise par exemple Google Analytics pour suivre et évaluer le comportement des visiteurs de son site Internet effectue un «suivi du comportement» soumis au RGPD pour autant qu'il localise les adresses IP. Ces dernières sont considérées comme des données personnelles.

Le RGPD concerne les clients qui achètent quels produits des transports publics?

A priori, le RGPD s'applique à la vente de produits visant explicitement des clients de l'UE, tels que les Swiss Travel Pass, les Interrail ou les offres touristiques. Il concerne également la banque de données des clients du Service direct, qui contient aussi des citoyens de l'UE.

Concrètement, quels changements y aura-t-il à l'égard du traitement des données clients?

Le traitement de données personnelles n'est plus permis qu'à certaines conditions. Le terme «traitement» est très général et comprend en particulier la collecte, la saisie, l'organisation, le classement, l'enregistrement, la modification, la lecture, la recherche, l'utilisation, la transmission, la suppression, la destruction, etc. des données. Le RGPD interdit tous ces processus, qu'ils soient manuels ou automatiques.

Quelles conditions doit remplir mon entreprise pour traiter les données personnelles conformément au droit?

Le traitement des données est licite à certaines conditions («motifs justificatifs»), parmi lesquelles::

- La personne concernée consent au traitement de ses données. Son consentement est soumis à des exigences élevées. La personne concernée doit être informée en détail au

préalable et donner volontairement son accord (voir question suivante sur les obligations). Le consentement doit par ailleurs être exprimé par une action univoque allant dans ce sens, p. ex. en cochant une case sur un site Internet.

- Le traitement est nécessaire à l'exécution d'un contrat conclu avec la personne concernée, p. ex. l'utilisation de l'adresse pour envoyer un abonnement.
- Le traitement est nécessaire au respect d'une obligation légale.
- Le traitement est nécessaire aux fins d'intérêts légitimes qui prévalent sur les intérêts de la personne concernée. Ce peut par exemple être le cas pour le marketing direct.

Quelles autres obligations doit satisfaire mon entreprise?

Le RGPD donne de lourdes obligations aux entreprises traitant les données. Ces obligations concernent notamment trois domaines centraux:

- Principes de traitement: Pour la personne concernée, il doit être clair dès le début que ses données seront traitées et à quelle fin (*transparence*). Seules les données nécessaires au traitement peuvent être collectées (*minimisation des données*) et elles ne peuvent l'être qu'à la fin mentionnée (*limitation des finalités*). En outre, les données ne doivent pas être conservées plus longtemps que nécessaire pour atteindre la finalité (*limitation de la conservation*).
- Information: Lors de la collecte des données personnelles, l'entreprise doit fournir de nombreuses informations. Celles-ci doivent être regroupées dans une politique de confidentialité écrite, mise à disposition spontanément et facilement accessible.
- Codes de conduite: Ces obligations contiennent une série de mesures favorisant la transparence, dont la tenue d'un registre de tous les traitements de données pertinents, une obligation de prouver que les dispositions du RGPD sont observées, une obligation d'annoncer les violations et une «*privacy by default*», par exemple par l'intermédiaire de réglages par défaut favorables au client dans les outils ou les applications. Les détails de ces obligations peuvent être consultés à l'adresse ch-direct.org/protection-donnees.

Pour quels clients et données clients doit s'appliquer le RGPD?

En théorie, les dispositions du RGPD ne doivent s'appliquer qu'à l'égard des clients domiciliés au sein de l'UE. Dans la pratique, il s'avérera pourtant difficile de distinguer les groupes de clients et de traiter les données différemment selon les cas. En outre, il faut s'attendre à ce que le législateur suisse durcisse également son droit de la protection des données pour le rapprocher de celui de l'UE.

En revanche, le RGPD exclut les données déjà anonymisées, comme les relevés de fréquence ou les comptages de voyageurs qui ne saisissent que des parcours et des types d'abonnement.

Quels sont les droits des clients concernés?

Le RGPD donne des droits étendus aux clients. Ces droits concernent principalement:

- une information accessible, compréhensible et complète quant au traitement des données de la part de l'entreprise (p. ex. dans une déclaration de protection des données),
- la correction de données erronées,
- la suppression de certaines données,

- la remise des données aux personnes qui en font la demande dans un format structuré et usuel.

Quelles mesures mon entreprise doit-elle prendre?

Les entreprises doivent agir au plus vite étant donné que des sanctions peuvent tomber déjà à partir du 25 mai. Chaque entreprise doit se demander si et dans quels cas elle est concernée par le nouveau règlement, mis à part les données personnelles du Service direct. Selon la situation, cette évaluation peut nécessiter l'aide d'un juriste.

À quoi faut-il faire attention lors du traitement des données des clients du SD?

Une attention particulière doit être accordée à l'utilisation des données clients à des fins de marketing. La KMP et la KVP ont décidé d'appliquer, dans ce cas, la procédure du «*soft opt-in*» dès l'entrée en vigueur du RGPD. Les clients actuels seront traités comme jusqu'ici, et les nouveaux clients à partir du 25 mai 2018 seront informés de façon transparente sur la réception d'offres et d'informations ainsi que sur les possibilités de désinscription. Aucun consentement explicite des clients n'est cependant nécessaire. Le «*soft opt-in*» peut uniquement être collecté durant le processus d'achat. L'attribut «*marketing permission*» correspondant est directement implémenté dans NOVA (attribut «publicité»). L'utilisation élargie des données reste possible avec la nouvelle procédure.

En ce qui concerne la mise en œuvre des demandes de renseignements et de suppression de données du SD, les CFF assurent la gestion en collaboration avec les entreprises de transport et garantissent une conception conforme à la loi.

Quels sont les effets de ces mesures pour mon entreprise?

Les entreprises de transport qui distribuent des produits du Service direct (abonnements et billets unitaires) doivent implémenter l'attribut «*marketing permission*» de NOVA dans tous les canaux sur lesquels elles vendent ces assortiments.

La désignation d'une personne chargée de la protection des données est recommandée à toutes les entreprises de transport afin de garantir les droits des clients. Cette personne transmet aux CFF (datenschutz@sbb.ch) les demandes de renseignement et de suppression de données de clients du Service direct si des données clients de NOVA sont concernées. De plus, les entreprises doivent elles aussi satisfaire ces demandes dans leurs propres systèmes conformément au RGPD.

*Remarque: chaque entreprise de transport peut collecter en sus sa propre «*marketing permission*». Le choix de la méthode («*opt-in*» ou «*soft opt-in*») est libre, mais un propre attribut doit impérativement être utilisé.*

Quelles sanctions peut craindre mon entreprise si elle viole le RGPD?

Des amendes salées peuvent être infligées en cas d'infractions au RGPD (jusqu'à 4 % du chiffre d'affaires annuel mondial ou vingt millions d'euros). Il est impossible de dire si et dans quelle mesure les autorités de surveillance prononceront des telles sanctions.

Qui peut m'aider? Où puis-je trouver plus d'informations?

Plusieurs notices sont disponibles à l'adresse ch-direct.org/protection-donnees. La page est continuellement actualisée.