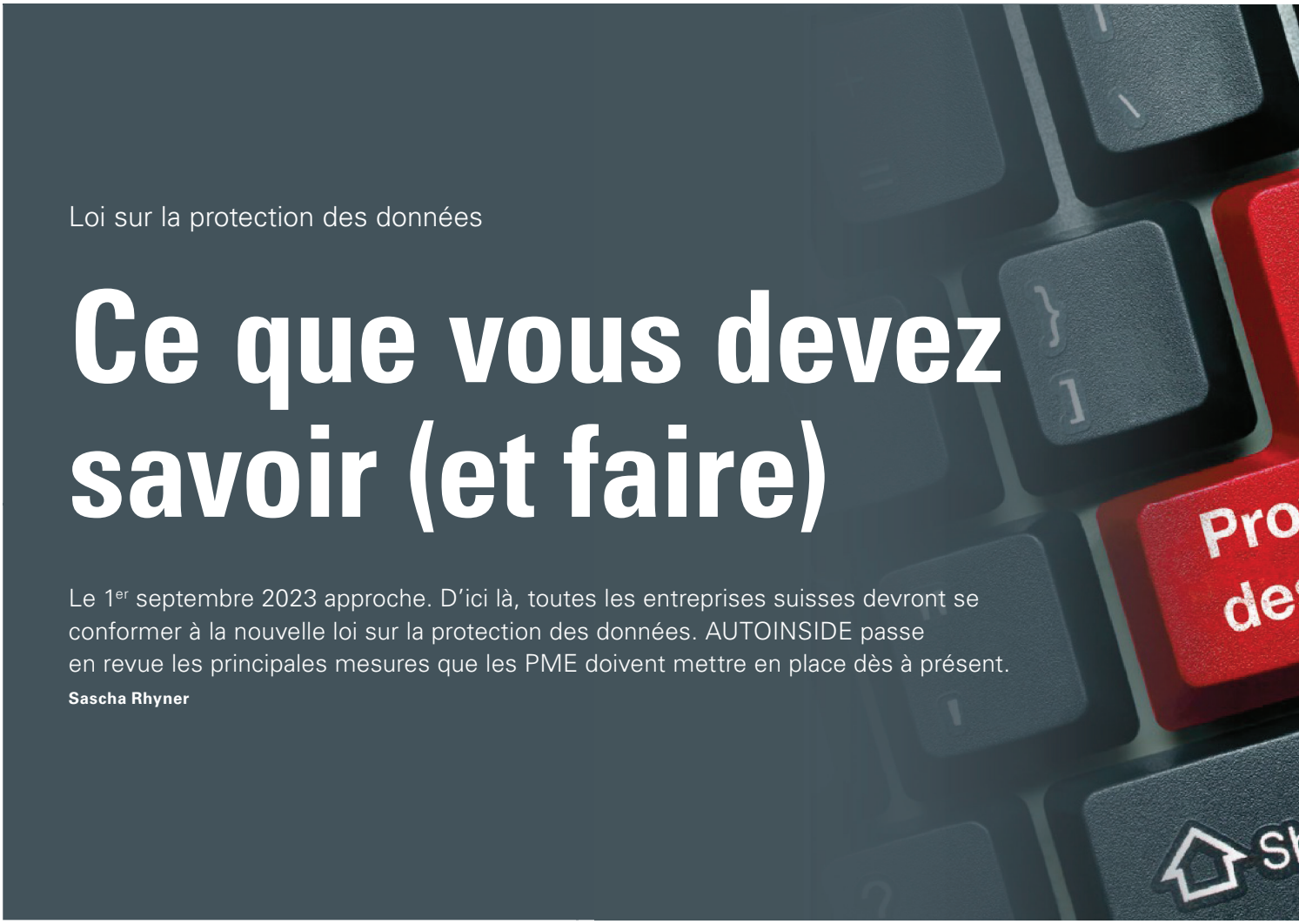

Loi sur la protection des données

Ce que vous devez savoir (et faire)

Le 1er septembre 2023 approche. D'ici là, toutes les entreprises suisses devront se conformer à la nouvelle loi sur la protection des données. AUTOINSIDE passe en revue les principales mesures que les PME doivent mettre en place dès à présent.

Sascha Rhyner

Pourquoi a-t-on besoin d'une nouvelle loi sur la protection des données ? L'une des raisons est l'adoption par l'UE, en mai 2018, du nouveau Règlement général sur la protection des données (RGPD), qui a également des conséquences en Suisse. La loi suisse sur la protection des données qui était en vigueur jusqu'ici datait de 1992. Le World Wide Web, développé au Cern de Genève, n'avait vu le jour que trois ans auparavant. En 1992, le premier téléphone mobile répondant à la norme GSM était présenté aux États-Unis, et le réseau Natel D lancé en Suisse. Dans le domaine de l'automobile, Fiat présentait la Cinquecento, héritière de la Topolino. Le 62e Salon de l'auto proposait pour la première fois une exposition spéciale sur le thème des véhicules électriques et solaires ; VW y présentait la Chico – alors considérée comme la future « Swatchmobile », BMW l'E1 et General Motors l'Impact. En d'autres termes, il s'est passé beaucoup de choses sur le plan technologique dans ce domaine depuis lors.

Mais quelles sont les principales nouveautés de la loi suisse sur la protection des données dans sa mouture de 2023 ? AUTOINSIDE passe en revue les points essentiels pour les PME.

Les « données sensibles » s'étendent

Les personnes physiques seront mieux protégées à l'avenir. Jusqu'ici, par exemple, seules les informations relatives à l'origine d'une personne, à la santé, à la religion ou aux opinions politiques étaient considérées comme des données sensibles. Désormais, les données génétiques, les données sur l'origine ethnique et les données biométriques (empreintes digitales, scan rétinien) seront elles aussi considérées comme sensibles.

Le « profilage » inscrit dans la LPD

Par « profilage », on entend des informations telles que le lieu de résidence d'une personne, sa situation économique, son état de santé, son âge, son rendement au travail ou ses passe-temps et autres intérêts. Ces informations permettent d'établir le profil précis d'une personne. Elles pourront continuer à être collectées, mais seulement avec la plus grande prudence. Cela signifie que la collecte de ces données ne doit pas porter atteinte aux droits de la personnalité. Lorsque les données permettent d'identifier les caractéristiques essentielles de la personnalité d'un individu, on parle de « profilage à risque élevé ». Dans ce cas, la nouvelle LPD exige le consentement explicite des personnes concernées.

Protection des données par défaut et dès la conception

Ces deux termes sont au cœur de la nouvelle LPD, il est donc important de connaître leur signification. La protection des données par défaut implique la mise en place de préréglages appropriés. L'objectif est notamment de protéger les utilisateurs qui ne sont pas versés dans la technique et ne tiennent pas suffisamment compte des paramètres de protection des données, par exemple sur les sites Web. L'une des manières de répondre à cette exigence est de concevoir une bannière de cookies qui permette à l'utilisateur de choisir activement certains cookies, mais où les coches nécessaires sont déjà paramétrées par défaut. Ce terme indique également que les

Photo : Shutterstock/médias de l'UPSA

Conseils

Il est essentiel que les PME examinent attentivement et, le cas échéant, adaptent leurs formulaires de commande et autres outils de collecte de données afin qu'ils soient conformes à la législation en septembre 2023. En tout état de cause, il est recommandé d'analyser minutieusement l'ensemble des données et de clarifier les points suivants :

- Quelles données sont collectées par qui (clients et employés) ?
- Lesquelles ne sont pas directement liées au service fourni ?
- Quelles données sont considérées comme sensibles ?
- Où sont-elles stockées ?
- La protection des données est-elle suffisante ?
- Qui a accès aux données à l'intérieur ou à l'extérieur de l'entreprise et cet accès est-il vraiment nécessaire ?
- Qui est responsable de la sécurité des données au sein de l'entreprise ? Cette personne est-elle suffisamment formée ?
- Quel processus intervient en cas de fuite de données et qui en est responsable ?

Dans le domaine de la protection des données, l'UPSA coopère avec l'entreprise spécialisée Impunix, qui vérifie et certifie la mise en œuvre intégrale de la loi suisse sur la protection des données, les directives des importateurs et des constructeurs ainsi que les recommandations de l'UPSA.

Plus d'infos sur : **impunix.ch**

données personnelles collectées doivent être conformes à la finalité poursuivie. Si l'on collecte davantage de données que nécessaire, les personnes concernées doivent en être informées et leur consentement doit être obtenu.

La protection des données dès la conception au sens de la LPD implique la mise en place de mesures techniques et organisationnelles au moment de la conception du traitement. Ce principe s'appuie sur l'idée que la meilleure façon de respecter la protection des données est de concevoir et de développer les logiciels et le matériel informatique de manière à prendre en compte dès le départ les mesures pertinentes en matière de protection des données.

Obligation de notification

En cas de violation de la protection des données personnelles, le responsable du traitement doit en informer immédiatement, si possible dans les 72 heures suivant le moment où il prend connaissance de la violation, l'autorité de surveillance, le Préposé fédéral à la protection des données et à la transparence. Par ailleurs, il doit également informer les personnes dont les données sont concernées. Le contenu de l'annonce aux autorités de surveillance est défini de manière détaillée dans la loi et comprend, outre les informations relatives à la violation, le nom et les coordonnées de l'interlocuteur au sein de l'entreprise. Si la violation est susceptible d'entraîner un risque élevé pour les droits et libertés individuels des personnes physiques, les personnes concernées doivent également en être informées.

Extension du devoir d'informer

Les obligations relatives à l'information sont considérablement renforcées. Désormais, les personnes doivent être informées de toute collecte de données les concernant. La nouvelle loi prescrit également de fournir des informations sur l'identité et les coordonnées du responsable du traitement, la finalité du traitement et les destinataires des données.

Pour clarifier un peu les choses, notons que les points suivants sont obligatoires :

- identité et coordonnées du responsable du traitement ;
- finalités du traitement ;
- en cas de transmission de données : les destinataires ou les catégories de destinataires ;
- en cas de transmission de données à l'étranger : l'État ou l'organisme international, ainsi que la garantie d'une protection adéquate des données ou, en l'absence d'une telle garantie, l'application d'une exception ;
- en cas de collecte indirecte de données (quand les données ne sont pas collectées auprès de la personne concernée) : les catégories de données traitées ;
- en cas de décision individuelle automatisée : toute personne peut exiger que la décision soit revue par une personne physique.

En cas de transmission de données à l'étranger, il convient d'obtenir le consentement de la personne concernée, et cette transmission doit s'avérer nécessaire en vertu du droit contractuel. En outre, en tant que PME, vous devez être en mesure de prouver que toutes les dispositions nécessaires en matière de protection des données sont respectées également dans le pays de destination.

La protection ne concerne que les personnes physiques

La révision de la LPD signifie que les entreprises et les organisations, c'est-à-dire les personnes morales, ne peuvent plus invoquer la loi. Le contenu de la protection ne s'applique plus qu'aux personnes physiques.

Planification des risques

Quiconque, en cas de dommage, n'est pas en mesure de prouver qu'il s'est préparé à l'avance est passible de sanctions. L'objectif est de réduire au maximum les risques liés à la collecte de données, et de pouvoir le démontrer en cas de doute.

Et attention : quiconque enfreint le devoir d'informer, fournit une information incomplète ou erronée sur la protection des données ou transmet des données personnelles illégalement à l'étranger encourt une amende pouvant atteindre 250 000 francs. Il est important de noter que l'amende ne frappera pas l'entreprise elle-même, mais la personne qui est effectivement responsable de la violation de la loi sur la protection des données. <