Les **nouveautés** dans le domaine de la **protection** des **données**

Frédérique Bensahel
[Avocate, FBT Avocats SA, Genève, Paris]

Aujourd'hui, la collecte de données constitue un outil de développement de choix pour les entreprises mais fait naître les plus grandes craintes du côté des particuliers. Dans un tel environnement, la question de la protection des données est devenu un enjeu majeur. La loi fédérale sur la protection des données (LPD), entrée en vigueur en 1993, constitue un garde-fou aux abus. Elle a pour but de réglementer le traitement et la divulgation des données, tant dans le secteur public que dans le secteur privé. Elle confère par ailleurs un droit fondamental au particulier, soit le droit d'avoir accès à ses données.

Parallèlement à l'attrait croissant des entreprises pour les données, les législateurs cherchent à protéger les personnes dont les données sont utilisées, le plus souvent à leur insu. La Suisse a lancé le chantier de la révision de la LPD en 2017. Celle-ci a abouti à une réforme dont la date d'entrée en vigueur a été fixée au 1er septembre 2023. L'objectif de cette réforme est d'assurer la garantie d'une meilleure protection de la sphère privée des personnes concernées par le traitement de leurs données personnelles en améliorant, d'une part, la transparence relative à ce traitement et, d'autre part, le droit d'accès à ces données, mais également de maintenir la compatibilité du droit suisse avec le droit européen et préserver ainsi la libre circulation des données, tout en garantissant la compétitivité de la Suisse.

Principales modifications apportées par la nouvelle teneur de la loi sur la protection des données

La LPD révisée prévoit une application immédiate, soit sans aucune période de transition pour une mise en conformité aux nouvelles obligations. Cela a pour conséquence que les entreprises touchées par les nouvelles dispositions – soit l'essentiel des entreprises suisses pour un certain nombre de dispositions – ont dû procéder à un ajustement aux nouvelles dispositions très rapidement.

Le premier grand changement introduit par cette révision est l'abandon par le législateur des règles sur la protection des données des personnes morales. Cet abandon n'aura toutefois que peu d'impact en pratique, puisque les données des personnes morales sont par ailleurs protégées par les articles 28 ss du Code civil suisse ainsi que par les lois en matière de concurrence déloyale et sur les droits d'auteur.

Un autre changement, portant plus à conséquence, est celui de la définition des données dites « sensibles ». La qualification de données sensibles est fondamentale dans le système de la LPD, ce type de données comportant une protection renforcée au motif que leur révélation peut avoir des conséquences préjudiciables sur la vie privée des personnes concernées. Les données sensibles selon la LPD révisée sont celles portant sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, celles portant sur la santé, la

Frédérique Bensahel

sphère intime ou l'origine raciale ou ethnique, les données génétiques, les données biométriques lorsqu'elles identifient une personne de manière univoque, les données sur des poursuites ou sanctions pénales ou administratives et, enfin, les données sur des mesures d'aide sociale. Au nombre des objectifs visés par l'élargissement de la définition des données sensibles, on trouve par exemple la volonté d'inclure les empreintes digitales ou vocales, dès lors qu'elles permettent l'identification d'une personne.

Suite aux progrès techniques et à l'apparition de nouvelles méthodes de traitement des données capables notamment d'enregistrer de grandes quantités de données, de les relier entre elles et de les analyser afin d'en tirer des informations sur les personnes à l'aide de procédés mathématiques et statistiques, la révision de la LPD remplace le terme de « profil de la personnalité » par le terme de « profilage ». Cette nouvelle dénomination intègre désormais tout type ou méthode de traitement des données, notamment les évaluations automatisées de certains aspects personnels d'une personne physique ; les « aspects personnels » dont il est question ici concernent notamment « le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements » de la personne physique en question. A côté du « profilage », la loi définit également désormais le « profilage à risque élevé », soit tout profilage qui entraîne un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée en ce qu'un tel profilage permet « d'apprécier les caractéristiques essentielles de la personnalité » d'une personne physique. Grâce à ces nouvelles qualifications, tout profilage par des organes fédéraux requerra une autorisation reposant sur une base légale.

Les principes de protection des données dès la conception *(« Privacy by design »)* et de protection des données par défaut *(« Privacy by Default »)* font leur apparition dans la nouvelle loi. Désormais, les entreprises seront tenues de mettre en place, par défaut et dès la conception, des mesures techniques et organisationnelles propres à respecter les prescriptions sur la protection des données.

La transparence dans le traitement des données est améliorée par la consolidation en faveur des personnes touchées du droit à l'accès des données et celle du droit d'être renseigné sur la question de savoir si des données personnelles sont collectées. Les nouvelles dispositions prévoient une obligation d'informer de manière préalable toute personne dont la collecte des données est envisagée. Le responsable du traitement des données est tenu de communiquer à la personne concernée les informations nécessaires à faire valoir ses droits. Le droit de toute personne concernée à recevoir ses données sous format électronique est également garanti. Enfin, chacun pourra également requérir la rectification et la suppression de ses données. Il est donc recommandé aux entreprises de prévoir une marche à suivre afin de pouvoir répondre rapidement à toute demande de renseignement et de suppression des données.

En cas de communication des données vers l'étranger, l'information sur la collecte de données doit mentionner les pays vers lesquels les données sont transférées et le niveau de protection offert ou les garanties qui ont été mises en place pour assurer une protection appropriée. La liste des pays offrant un niveau de protection adéquat figure dorénavant dans l'ordonnance d'application de la loi ; pour les pays qui n'y figurent pas, un transfert des données personnelles vers ceux-ci n'est possible que s'il existe un niveau de protection adéquat dans le pays de destination des données, ce qui peut résulter, en substance, d'un traité international, de clauses contractuelles de protection des données préalablement communiquées au Préposé fédéral à la protection des données et à la transparence (PFPDT), de garanties spécifiques élaborées par un organe fédéral et communiquées au PFPDT, de clauses type de protection des données préalablement approuvées, établies ou reconnues par le PFPDT, ou encore de règles d'entreprise contraignantes préalablement approuvées ; des dérogations sont possibles dans certains cas particuliers limitativement énumérés. Il s'ensuit que les entreprises devront donc déterminer vers quels pays les données sont transférées (en cas, par exemple, de stockage sur un cloud), déterminer le niveau de protection offert par ce pays, déterminer – pour le cas où le pays en question ne figure pas sur la liste du Conseil fédéral – si d'autres garanties sont en place, ou déterminer si une exception est justifiée au regard du catalogue limitatif prévu par la loi.

On relèvera encore, à l'heure des *robot advisors*, l'obligation nouvelle d'informer les personnes concernées de toute décision prise exclusivement sur la base d'un traitement de données personnelles entièrement automatisé. En d'autres termes, la LPD révisée impose une obligation d'information lorsqu'une décision est prise exclusivement par un logiciel.

Enfin, les entreprises devront établir et tenir un registre des activités de traitement des données, lequel devra être régulièrement mis à jour. Les entreprises de moins de 250 collaborateurs, dont le traitement des données présente un faible risque d'atteinte à la personnalité, sont toutefois exemptée de cette mesure. Cette exemption n'est possible que si le traitement des données effectué par l'entreprise ne porte pas sur des données sensibles à grande échelle ni constitue un profilage à risque élevé. Pour les entreprises exemptées, l'opportunité de tenir un registre des activités de traitement des données doit toutefois être analysée en vue de déterminer l'utilité d'un tel registre – même en l'absence d'une obligation légale – ainsi que les conditions d'exemption.

La révision encourage la responsabilisation des personnes en charge du traitement des données en prévoyant notamment la possibilité pour les associations professionnelles et les associations économiques de rédiger leur propre code de conduite et de le soumettre au PFPDT. L'aval de ce dernier établira la présomption légale que le comportement défini dans le code respecte la protection des données.

La révision instaure une véritable obligation de procéder à des analyses d'impact, à l'instar de celles déjà prévues pour les organes fédéraux. Ces analyses ne sont obligatoires qu'en cas de traitement de données susceptible d'entraîner un risque élevé pour les droits de la personnalité ou les droits fondamentaux des personnes concernées. Il est toutefois possible de renoncer à de telles analyses d'impact en cas de certification, par un organisme de certification agréé ou indépendant, du système, produit ou service utilisé, ou en cas de respect du code de conduite agréé. Lorsqu'elle doit être effectuée, l'analyse d'impact comportera une description du traitement envisagé, une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée, ainsi que les mesures prévues pour protéger sa personnalité et ses droits fondamentaux. Aucune méthodologie particulière n'étant prévue dans la loi, il est donc conseillé de suivre les recommandations des autorités de contrôle européennes.

Enfin, la révision instaure une obligation générale d'informer le PFPDT et la personne concernée, dans les meilleurs délais, de toute violation de la sécurité entraînant de manière vraisemblable un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées. Jusqu'à présent, ce devoir d'annonce n'existait que pour les établissements soumis à la surveillance de la FINMA.

Conclusion

La nouvelle teneur de la LPD a pour objectif de renforcer la confiance des consommateurs dans le traitement de leurs données personnelles. Ce renforcement a cependant un coût pour les responsables de traitement des données, soit généralement les entreprises. Toutefois, les entreprises suisses qui offrent des services dans les Etats membres de l'Union européenne soumis au règlement (UE) 2016/679 ont déjà fait le plus gros de l'effort dans la mesure où l'implémentation de ce règlement implique déjà pour l'essentiel une mise en conformité avec les nouvelles dispositions de la LPD.

New **developments** in **data protection**

Frédérique Bensahel
[Attorney-at-Law, FBT Avocats SA, Geneva, Paris]

Today, data collection is a key development tool for businesses but it is also a source of great concern for individuals. In such an environment, data protection has become a major issue. The Federal Data Protection Act (DPA), which came into force in 1993, is a safeguard against abuse. Its purpose is to regulate the processing and disclosure of data both in the public and private sectors. It also confers a fundamental right on individuals: the right to access their own data.

At the same time as companies are increasingly attracted by data, legislators are seeking to protect the people whose data is used, usually without their knowledge. Switzerland launched the revision of the Data Protection Act in 2017. The result is a reform that will come into force on 1st September 2023. The aim of this reform is to guarantee better protection of the private sphere of people concerned by the processing of their personal data by improving, on the one hand, the transparency of this processing and, on the other hand, the right of access to this data, but also to maintain the compatibility of Swiss law with European law and thus preserve the free circulation of data, while guaranteeing Switzerland's competitiveness.

Main changes introduced by the new content of the Data Protection Act

The revised DPA provides for immediate application, i.e. without any transition period for compliance with the new obligations. As a result, companies affected by the new provisions – i.e. the majority of Swiss companies for a certain

number of provisions – have had to adjust to the new provisions very quickly.

The first major change introduced by this revision is that the legislator has abandoned the rules on data protection for legal entities. However, this will have little impact in practice, since the data of legal entities is otherwise protected by Articles 28 et seq. of the Swiss Civil Code and by the laws on unfair competition and copyright.

Another more significant change is the definition of "sensitive" data. The definition of sensitive data is fundamental to the DPA system, as this type of data is subject to enhanced protection on the grounds that its disclosure may have harmful consequences for the privacy of the individuals concerned. Sensitive data under the revised DPA includes data relating to religious, philosophical, political or trade union opinions or activities, data relating to health, privacy or racial or ethnic origin, genetic data, biometric data where it uniquely identifies a person, data relating to criminal or administrative proceedings or sanctions and, lastly, data relating to social welfare measures. One of the aims of extending the definition of sensitive data is to include fingerprints or voice prints, where these can be used to identify a person.

As a result of technical progress and the emergence of new data processing methods capable in particular of recording large quantities of data, linking them together and analysing them in order to derive information about individuals using mathematical and statistical processes, the revision of the DPA replaces the term "personality profile" with the term "profiling". This new term now includes any type or method of data processing, in particular automated assessments of certain personal aspects of a natural person; the "personal aspects" referred to here include "work performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements" of the natural person in question. In addition to "profiling", the law now also defines "high-risk profiling", i.e. any profiling that entails a high risk for the personality or fundamental rights of the data subject in that such profiling makes it possible to "assess the essential personal characteristics" of a natural person. Thanks to these new qualifications, all profiling by federal bodies will require authorisation with a legal basis.

The principles of *"Privacy by design"* and *"Privacy by default"* have been introduced in the new law. From now on, companies will be required to put in place, by default and right from the design stage, technical and organisational measures to comply with data protection regulations.

Transparency in data processing has been improved by consolidating the right of data subjects to access their data and the right to be informed as to whether or not personal data is being collected. The new provisions lay down an obligation to provide prior information to any person whose data is to be collected. The data controller is obliged to provide data subjects with the information they need to exercise their rights. The right of all data subjects to receive their data in electronic format is also guaranteed. Lastly, anyone may also request that their data be rectified or deleted. It is therefore recommended that companies establish a procedure for responding rapidly to any request for information or deletion of data.

Where data is transferred abroad, the information on data collection must mention the countries to which the data is transferred and the level of protection offered or the safeguards that have been put in place to ensure adequate protection. The list of countries offering an adequate level of protection is now set out in the ordinance implementing the Act; for countries that are not on the list, personal data may only be transferred to them if there is an adequate level of protection in the country of destination, which may result, in substance, from an international treaty, contractual data protection clauses communicated in advance to the Federal Data Protection and Information Commissioner (FDPIC), specific guarantees drawn up by a federal body and communicated to the FDPIC, standard data protection clauses previously approved, drawn up or recognised by the FDPIC, or binding company rules previously approved; derogations are possible in certain specific cases, which are listed exhaustively. As a result, companies will have to determine to which countries the data is transferred (in the case, for example, of storage on a cloud), determine the level of protection offered by that country, determine – if the country in question is not on the Federal Council's list – whether other guarantees are in place, or determine whether an exception is justified in the light of the restrictive catalogue provided by law.

In the age of *robot advisors*, there is also a new obligation to inform data subjects of any decision taken exclusively on the basis of fully automated processing of personal data. In other words, the revised DPA imposes a duty to inform when a decision is taken exclusively by a software.

Finally, companies will have to establish and maintain a register of data processing activities, which will have to be regularly updated. Companies with fewer than 250 employees, whose data processing presents a low risk of damage to personality, are exempt from this measure. This exemption is only possible if the data processing carried out by the company does not involve large-scale sensitive data or constitute high-risk profiling. For exempted companies, the appropriateness of keeping a register of data processing activities must be analysed in order to determine the usefulness of such a register – even in the absence of a legal obligation – and the conditions for exemption.

The revision encourages those responsible for data processing to take responsibility for their actions, in particular by allowing professional and business associations to draw up their own code of conduct and submit it to the FDPIC. The latter's approval will establish the legal presumption that the behaviour defined in the code complies with data protection.

The revision introduces a genuine obligation to carry out impact assessments, along the lines of those already provided for federal bodies. These analyses are only compulsory in the case of data processing likely to entail a high risk for the personal rights or fundamental rights of the data subjects. However, such impact analyses may be waived if the system, product or service used is certified by an approved or independent certification body, or if the approved code of conduct is complied with. Where it must be carried out, the impact assessment will include a description of the processing envisaged, an assessment of the risks to the data subject's personality or fundamental rights, and the measures planned to protect the data subject's personality and fundamental rights. As no specific methodology is laid down in the law, it is advisable to follow the recommendations of the European supervisory authorities.

Finally, the revision introduces a general obligation to inform the FDPIC and the data subject, as soon as possible, of any breach of security that is likely to result in a high risk to the personality or fundamental rights of the data subject. Until now, this duty to report existed only for institutions subject to the supervision of the FINMA.

Conclusion

The aim of the new version of the DPA is to strengthen consumer confidence in the processing of their personal data. However, this comes at a cost to the data controllers, i.e. generally the companies. However, Swiss companies offering services in European Union member states subject to the EU Regulation 2016/679 have already made the greatest effort, as the implementation of this regulation essentially already involves compliance with the new provisions of the DPA. ■