Philippe Ehrenström

WEKA

La protection des données de A à Z

L'essentiel par mots clés

CIP-Notice abrégée de la deutsche Bibliothek

La protection des données de A à Z

Auteur: WEKA Business Media SA

Direction de projet: Birgitt Bernhard-Postma

WEKA Business Media AG, Suisse

WEKA Business Media AG
Hermetschloostr. 77, CH-8048 Zurich
Téléphone 044 434 88 88, Téléfax 044 434 89 99
www.weka.ch

Zurich • Kissing • Paris • Vienne

ISBN 978-3-297-02253-5

1er édition 2022

Impression: CPI books GmbH, Leck / Layout: Dimitri Gabriel / Composition: Dimitri Gabriel

BBOOKS BUSINESS BOOKS *Un problème? **Pas de problème!***

Table des matières

Introduction

La loi fédérale du 19 juin 1992 sur la protection des données (LPS; RS 235.1) fêtera probablement son trentième anniversaire quand elle sera remplacée, début 2023, par un nouveau texte, considérablement remanié et très largement inspiré du droit européen (nouvelle loi fédérale du 25 septembre 2020 sur la protection des données [nLPD; FF 2020 7397]).

La Suisse ne serait bien évidemment pas la Suisse si ces remaniements n'avaient pas été que très partiels dans certains domaines, et l'inspiration du droit européen très parcellaire ailleurs. Mais le fait est là, il nous reste environs une année avant un changement de système qui va introduire des obligations et des modifications du droit et des pratiques très considérables.

D'aucuns disent que ces changements ne seraient, somme toute, que très modestes, dans la mesure où une bonne partie du travail d'adaptation aurait déjà été fait lors de l'entrée en vigueur du Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, dit règlement général sur la protection des données (RGPD), eu égard à l'application extraterritoriale dudit règlement dans certaines circonstances. C'est oublier que beaucoup d'acteurs, sur le marché suisse, sont orientés, précisément, sur le marché intérieur, et que tous n'ont pas eu les ressources (ou l'intérêt) pour effectuer ce «reset» en matière de protections des données imposé à certain (mais pas à tous) par le droit européen. Or là, il va être difficile d'ignorer l'exercice: le droit national l'impose, il va s'appliquer à tout le monde et la nLPD va introduire des obligations et nouveautés qui vont devoir être maîtrisées et intégrées rapidement.

Le but de ce dictionnaire, vous l'aurez compris, est donc d'aider les acteurs à s'adapter au nouveau droit suisse de la protection des données en les familiarisant avec la langue, les concepts et les nouveautés de la nLPD. Les entreprises, les particuliers, vont devoir faire un effort considérable d'adaptation au nouveau droit. Il n'est donc pas inutile d'avoir un lexique, des explications simples rangées par ordre alphabétique et des exemples pour progresser et passer le cap.

Liste des principaux textes de loi et abréviations

Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst.; RS 101)

Code de procédure civile (RS 272; CPC)

Code des obligations (RS 229; CO)

Convention européenne des droits de l'homme (CEDH)

Loi fédérale du 19 juin 1992 sur la protection des données (LPD; RS 235.1)

Nouvelle loi fédérale du 25 septembre 2020 sur la protection des données, adoptée le 25 septembre 2020, et qui devrait renter en vigueur début 2023 (nLPD; FF 2020 7397)

Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD; RS 235.11)

Avant projet d'Ordonnance relative à la loi fédérale sur la protection des données, mis en consultation jusqu'au 14 octobre 2021 (P – OLPD)

Loi fédérale du 17 décembre 2004 sur le principe de transparence dans l'administration (Loi sur la transparence, LTrans; RS 152.3)

Ordonnance du 18 août 1993 relative à la loi sur le travail (OLT3; RS 822.113)

Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données [RGPD])

Bibliographie indicative

Bruno BAERISWYL/Kurt PÄRLI, Handkommentar Datenschutzgesetz (DSG), Berne, 2015

Eva CELLINA, La commercialisation des données personnelles, Genève-Zurich-Bâle, 2020

Livio DI TRIA, L'analyse d'impact relative à la protection des données (AIPD) en droit européen et suisse, sic ! 3/2020, pp. 119 et ss.,

Benjamin DOMENIG/Christian MITSCHERLICH, Datenschutzrecht für Schweizer Unternehmen, Berne, 2019

Martin ECKERT/Eric Neuenschwander, Datenschutzrecht, Zurich, 2019

Sylvain METILLE (éd.), Le droit d'accès, Berne, 2021

Sylvain METILLE, Le traitement de données personnelles sous l'angle de la (nouvelle) loi fédérale sur la protection des données du 25 septembre 2020, SJ 2021 II 1 et ss.

Philippe MEYER, Protection des données, Berne, Stämpfli, 2011

Philippe MEYER, Droit des personnes, 2e éd., Genève-Zurich-Bâle, 2021

David ROSENTHAL, La nouvelle loi sur la protection des données, in: Jusletter 16 novembre 2020

A

Lettre A

Analyse d'impact

L'art. 22 nLPD introduit dans notre droit l'analyse d'impact relative à la protection des données personnelles [ci-après AIPD] (en droit européen: art. 35 RGPD).

L'AIPD, sous la forme d'une auto-évaluation, est un instrument préventif, un outil de compliance pour valider et justifier les traitements de données plus sensibles du point de vue du respect de la protection des données.

A teneur de l'art. 22 al. 1 nLPD, lorsque le traitement de données envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données personnelles. S'il envisage d'effectuer plusieurs opérations de traitement semblables, il peut établir une analyse d'impact commune.

L'existence d'un risque élevé, en particulier lors du recours à de nouvelles technologies, dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Un tel risque existe notamment dans les cas suivants: a. traitement de données sensibles à grande échelle; b. surveillance systématique de grandes parties du domaine public.

La notion de risque élevé est à la fois complexe et floue. Le risque est la combinaison de sa probabilité d'occurrence et de la gravité du dommage en résultant. Ainsi, si la première est probable ou très probable, et la seconde importante à grande, alors il y aura vraisemblablement un «risque élevé» pour la personnalité et les droits fondamentaux de la personne concernée.

L'analyse d'impact contient 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 (art. 22 al. 3 nLFD). La loi ne contient pas méthodologie particulière. Il conviendra de s'inspirer de ce qui est conseillé par les autorités de contrôle européennes [cf. les critères contenus dans ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679, 4 octobre 2017; de la même manière, selon l'art. 35 al. 4 RGPD, les autorités de contrôle sont tenues d'établir et de publier des listes «positives» de types d'opération pour lesquels une AIPD est requise].

Le responsable du traitement privé est délié de son obligation d'établir une analyse d'impact s'il est tenu d'effectuer le traitement en vertu d'une obligation légale.

Le responsable du traitement privé peut renoncer à établir une analyse d'impact lorsqu'il recourt à un système, un produit ou un service certifié conformément à l'art. 13 nLPD

pour l'utilisation prévue ou qu'il respecte un code de conduite au sens de l'art. 11 nLPD remplissant les conditions suivantes: a. il repose sur une analyse d'impact relative à la protection des données personnelles; b. il prévoit des mesures pour protéger la personnalité et les droits fondamentaux de la personne concernée; c. il a été soumis au Préposé fédéral à la protection des données et à la transparence (PFPDT).

L'art. 23 nLPD règle les cas où le responsable de traitement doit consulter au préalable le PFPDT.

Le responsable du traitement consulte ainsi le PFPDT préalablement au traitement lorsque l'analyse d'impact relative à la protection des données révèle que, malgré les mesures prévues par le responsable du traitement, le traitement envisagé présente encore un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 23 al. 1 nLPD).

Le PFPDT communique au responsable du traitement ses objections concernant le traitement envisagé dans un délai de deux mois, délai qui peut encore être prolongé d'un mois lorsqu'il s'agit d'un traitement de données complexe (art. 23 al. 2 nLPD). Si le PFPDT a des objections concernant le traitement envisagé, il propose au responsable du traitement des mesures appropriées (art. 23 al. 3 nLPD).

Le responsable du traitement privé peut renoncer à consulter le PFPDT s'il a consulté son conseiller à la protection des données (art. 23 al. 4 nLPD).

Concernant la forme et la conservation de l'AIPD, l'art. 18 de l'avant projet d'Ordonnance relative à la loi fédérale sur la protection des données, mis en consultation jusqu'au 14 octobre 2021 (P – OLPD) [https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-84103.html] prévoit que le responsable du traitement consigne par écrit l'analyse d'impact relative à la protection des données personnelles; l'AIPD est conservée pendant deux ans après la fin du traitement des données.

Le rapport explicatif au nouveau projet d'ordonnance précise que la forme écrite comprend à la fois les documents papiers et ceux sous forme électronique. Elle est particulièrement importante pour prouver qu'une analyse d'impact a bien été faite. Par ailleurs, si l'analyse d'impact relative à la protection des données doit être conservée après que le traitement des données a eu lieu, c'est parce qu'elle constitue un instrument central de la législation sur la protection des données. Elle peut notamment se révéler importante lorsqu'il faut faire la lumière sur une violation de la sécurité des données ou évaluer la punissabilité d'un comportement. Elle fournit donc des informations sur la façon dont on a évalué les risques pour la personnalité et les droits fondamentaux, et les mesures qui ont été prises. (Révision totale de l'ordonnance relative à la loi fédérale sur la protection des données, Rapport explicatif relatif à la procédure de consultation, 23 juin 2021, pp. 30–31).