La protection des données en entreprise

Special Dossier

WEKA

Auteurs

Lukas Lezzi, docteur en droit, CIPP/E, CIPM, CAS Forensics, est avocat indépendant à Zurich (LezziLegal). Il a fait ses études à Zurich et a rédigé une thèse en droit des marchés financiers. Ses domaines de prédilection sont la protection des données et le droit des marchés financiers.

Renisa Lajqi travaille comme collaboratrice chez LezziLegal dans le cadre de ses études universitaires. Elle étudie le droit à Zurich.

Shqipe Beluhli, Mlaw, travaille comme juriste chez LezziLegal. Elle a étudié à Zurich et à Lausanne. Elle s›occupe principalement de projets relevant du droit de la protection des données et de la réglementation.

Luciana Viganò, Mlaw, travaille comme juriste chez LezziLegal. Elle a fait ses études à Bâle. Chez LezziLegal, elle conseille les clients en matière de protection des données et de droit des contrats.

Impressum

La protection des données en entreprise

Special Dossier

Auteurs Lukas Lezzi, Mlaw Shqipe Beluhli, Renisa Lajqi & Mlaw Luciana Viganò

Direction de projet Birgitt Bernhard **Traduction** Nicolas Turberg **Mise en page/composition** Sarah Rutschmann

WEKA Business Media SA, Hermetschloostrasse 77, 8048 Zürich, Tel. 044 434 88 34
info@weka.ch, www.weka.ch, www.weka-library.ch

Zurich • Kissing • Paris • Vienne

SD8135-2099-202504

Table des matières

1

Introduction

Avec l'entrée en vigueur de la révision totale de la loi sur la protection des données (LPD) le 1er septembre 2023, la Suisse a fait un pas décisif en direction des normes modernes de protection des données. Le présent guide ne met pas seulement en lumière les aspects juridiques de la nouvelle loi sur la protection des données mais souligne également la nécessité d'intégrer la protection des données dans la gouvernance même des entreprises.

Les entreprises se doivent d'avoir une perspective globale de ce phénomène et d'analyser tous les domaines pertinents de leur structure de gouvernance. Dans ce contexte, il est important de comprendre les interactions entre la LPD et les autres politiques, processus et structures de l'entreprise tant il est clair que la question de la protection des données doit être prise en compte dans pratiquement tous les secteurs de l'entreprise.

Le présent dossier a pour objectif de fournir aux entreprises un guide pratique leur permettant de mettre en œuvre de la manière la plus pragmatique possible les exigences de la nouvelle loi sur la protection des données aux différents niveaux de leur organisation. Il est utile de noter que seuls les points les plus importants concernant la mise en œuvre des exigences susmentionnées sont abordés du point de vue des auteurs et que la LPD n'est, de ce fait, pas commentée dans son ensemble.

Voici quelques définitions pour que l'on sache d'emblée de quoi il s'agit:

a) **Responsable du traitement:** la personne privée ou l'organe fédéral qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles.

b) **Données personnelles:** données personnelles: toutes les informations concernant une personne physique identifiée ou identifiable (ci-après «les personnes concernées»). Il peut s'agir, par exemple, des nom, adresse électronique, lieu de résidence et numéro de téléphone d'une personne.

c) **Données personnelles sensibles (données sensibles):** celles-ci constituent une sous-catégorie des données personnelles. Toutes les données suivantes nécessitent une protection particulière et un traitement plus strict:
   - les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales;
   - les données sur la santé, la sphère intime ou l'origine raciale ou ethnique,
   - les données génétiques;

- les données biométriques identifiant une personne physique de manière univoque;
- les données sur des poursuites ou sanctions pénales et administratives et
- les données sur des mesures d'aide sociale

d) **Traitement:** toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données;

e) **Sous-traitant:** une personne physique, une personne morale ou un organisme public qui traite des données personnelles pour le compte et sur les instructions du responsable du traitement. Par exemple, un prestataire de services cloud qui héberge des données personnelles pour l'entreprise.

f) **Profilage:** toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;

g) **Profilage à risque élevé:** tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique;

2 Mise en œuvre concrète au sein de l'entreprise

Il est en tous les cas recommandé de prévoir une petite organisation de projet pour la mise en œuvre de la LPD dans l'entreprise. L'ampleur et la poursuite d'une telle entreprise sont bien entendu très individuelles et dépendent de différents facteurs:

- Quelle est l'importance des traitements de données pour l'entreprise, en particulier les traitements de données présentant des risques élevés, par exemple les décisions automatisées, le traitement de données personnelles sensibles, les décisions automatisées, etc.?

– Existe-t-il déjà un cadre de protection des données pour le Règlement général européen sur la protection des données (RGPD), qui pourrait être complété par les exigences de la LPD?
– Quelles sont les ressources qui pourraient être mises à disposition?

En principe, la direction de l'entreprise devrait dans tous les cas être impliquée en tant que partie prenante dans le cadre d'un tel projet, la protection des données touchant en fin de compte toutes les parties d'une entreprise. Le responsable interne de la protection des données (Data Protection Officer/DPO) et les représentants de la sécurité de l'information (Information Security) devraient également participer au projet à titre de soutien, pour autant que ces fonctions existent.

Pour les petites entreprises, il est recommandé de faire appel à un soutien externe, tout au moins de manière ponctuelle, lors de la phase de conception du projet. La réalisation d'un tel projet peut ensuite très bien être effectuée à l'interne.En règle générale, il est recommandé de ne pas faire réaliser un tel projet entièrement par des personnes externes à l'entreprise (par exemple en faisant appel à un cabinet d'avocats ou à une entreprise de conseil), car une fois le projet terminé, les nouveaux processus devront effectivement être acceptés et expérimentés à l'interne. Cet objectif ne peut être atteint que si les nouveaux processus sont également élaborés au sein de l'entreprise.