privatim
die schweizerischen datenschutzbeauftragten
les commissaires suisses à la protection des données
gli incaricati svizzeri della protezione dei dati

AIDE-MEMOIRE

Utilisation des médias sociaux par les organes publics en conformité avec la protection des données

I. Introduction

Cet aide-mémoire s'adresse aux organes publics qui sont soumis à la législation sur la protection des données cantonale et qui utilisent des médias sociaux comme Twitter et Facebook.

Twitter et Facebook sont utilisés en tant que plateformes pour la publication et pour l'échange directs entre citoyennes et citoyens. Plusieurs acteurs (opérateur de plateforme, provider, organe public en tant qu'utilisateur, tiers) peuvent traiter des informations à des finalités diverses. En outre, des tiers non concernés peuvent être atteints par le traitement des données. Ci-dessous, nous allons détailler la situation juridique ainsi que les mesures à prendre pour une utilisation conforme à la protection des données de Twitter et de Facebook. En principe, ce document peut également s'appliquer à d'autres médias sociaux comme LinkedIn, XING, Myspace, Youtube etc. Il faudra toutefois vérifier concrètement si des adaptations sont nécessaires pour l'utilisation de ces autres médias sociaux.

D'éventuelles démarches se situant an amont de l'ouverture d'un compte des médias sociaux ne font pas l'objet du présent document, dans la mesure où elles ne concernent pas directement la protection des données (élaboration d'une stratégie, directives pour des collaborateurs, planification des ressources etc.).

II. En droit

Les organes publics qui publient des documents et qui communiquent de façon interactive sur Twitter et/ou sur Facebook doivent respecter les conditions découlant de la loi sur la protection des données. Demeurent réservées les dispositions cantonales qui doivent être respectées avant l'ouverture de tels comptes de médias sociaux (comme par exemple des obligations de contrôle préalable).

privatim
die schweizerischen datenschutzbeauftragten
les commissaires suisses à la protection des données
gli incaricati svizzeri della protezione dei dati
c/o Datenschutzbeauftragter des Kantons Zürich
Postfach, CH-8090 Zürich
Tel. +41 (43) 259 39 99, Fax +41 (43) 259 51 38
geschaeftsstelle@privatim.ch, www.privatim.ch

1. Ouverture d'un "compte" („Account“)

L'utilisation de plateformes de médias sociaux se base sur une relation juridique entre l'opérateur de la plateforme et l'organe public. Cette relation contractuelle comporte des éléments de différents types de contrats. Le contrat prend effet avec l'ouverture d'un "compte" et l'acceptation des conditions générales, préalablement formulées par l'opérateur. Ces conditions générales, dont l'acceptation découle de l'ouverture du «compte», peuvent être périodiquement modifiées, de manière spontanée, unilatérale et sans qu'une telle modification ne soit annoncée à l'organe public. L'opérateur de la plateforme peut aussi sauvegarder, analyser et utiliser les informations à ses propres fins, sans que l'organe public ne puisse influer sur ce comportement.

2. Publications

La communication de données suppose une base légale ou le consentement de la personne concernée. La base légale permettant la publication d'informations se trouve dans la loi sur la protection des données, la loi sur l'information ainsi que dans des actes normatifs régissant des domaines spécifiques. Quand une personne consent à une publication, ce consentement doit avoir été donné en connaissance de toutes les conséquences possibles liées à la publication dans l'internet («consentement éclairé»).

Le secret de fonction et des devoirs de discrétion particuliers, comme par exemple le secret fiscal, peuvent s'opposer à une éventuelle publication.

Comme les utilisateurs sont forcés de divulguer des données personnelles pour avoir accès à de telles informations, les organes publics doivent mettre à disposition d'autres moyens d'information pour ceux qui ne veulent pas se servir des médias sociaux.

3. Communication interactive

L'utilisation de médias sociaux ne doit pas remplacer l'activité administrative, mais elle peut offrir une plateforme supplémentaire d'information rapide et détaillée sur des questions importantes. Les médias sociaux ne sont pas adaptés l'exercice du pouvoir public. L'échange interactif doit être restreint à un minimum, car la collecte, la sauvegarde et le traitement ultérieur de données (souvent très complètes) est délicat. Si on dépasse l'échange d'informations banales ou si on est en présence d'une application du droit à un cas particulier, alors il faut renvoyer les parties en cause aux canaux usuels de la communication administrative (demande écrite, formulaire de contact etc.).

III. Responsabilité

L'organe public est responsable des contenus qu'il fait figurer sur la plateforme. Une responsabilité existe aussi pour les commentaires d'utilisateur. Il s'en suit une obligation de gérer activement la plateforme.

Les informations doivent régulièrement être contrôlées, afin de détecter des contenus pouvant porter atteinte à la personnalité ou posant des problèmes sur le plan pénal. En outre, il convient de lire les commentaires des utilisateurs, afin de vérifier s'ils donnent lieu à une activité administrative. Si, par exemple, une demande d'accès à des informations est faite auprès de l'organe public, celui-ci doit répondre de manière appropriée (par exemple par courriel, si cela concerne des données personnelles ou par courrier postal, si la réponse contient des données sensibles). Un devoir d'agir des organes publics peut exister si des fausses informations sont diffusées et que des tiers pourraient être influencés (par exemple, si avant une votation des contenus erronés sont publiés sur la plateforme).

L'organe public doit faire connaître, par publication sur la plateforme, la réglementation qui régit la gestion de son «compte». Dans ce cadre, les utilisateurs peuvent être avisés des risques que l'utilisation peut faire naître pour leurs droits de la personnalité et ils peuvent être informés des moyens permettant d'éviter ces risques, par une recommandation de comportement.

IV. Mesures

1. Mesures préalables

Avant l'ouverture d'un compte, l'organe public doit notamment se soucier des points suivants:

- le choix des médias sociaux
- la façon d'utiliser les médias sociaux
- le but de l'utilisation
- les implications sur les utilisateurs, liées à la mise en place et à la mise en œuvre des communications interactives
- les mesures à prendre, afin de permettre une utilisation conforme à la protection des données

L'utilisation de plateformes par les organes publics doit être planifiée soigneusement, lorsqu'elle découle sur des traitements de données sensibles (par exemple dans le cadre d'une clinique psychiatrique ou d'une prison). Des mesures pertinentes, par exemple le blocage de la communication interactive, doivent faire partie de la planification.

2. Règles d'utilisation

L'organe public doit renseigner sur les aspects généraux de l'utilisation, notamment sur:

- la personne de contact et son adresse
- la nature, l'ampleur et le but de l'utilisation de la plateforme
- les périodes de «monitoring» (normalement durant les heures ouvrables)

- les règles liées à la gestion (réponse aux commentaires uniquement dans le cadre de la mission légale, réserve de la suppression de contenus problématiques sur le plan pénal et/ou portant atteinte à la personnalité, la sauvegarde de logfiles dans des cas problématiques, procédure d'effacement etc.)

Il faut aussi informer sur les risques liés par exemple à la sauvegarde, à l'exploitation et à la réutilisation des données des utilisateurs par l'opérateur.

3. Monitoring

Un "compte" doit être géré activement par l'organe public. Les commentaires doivent être lus en portant une attention particulière aux points suivants:

- les commentaires problématiques sur le plan pénal et/ou civil
- les requêtes donnant lieu à une activité administrative
- les fausses informations qui se réfèrent à des publications de l'organe public et qui influencent des tiers

Pour une telle gestion, il existe des programmes spécifiques. Des commentaires à contenu politique ou contenant d'autres informations sensibles ne peuvent faire l'objet que d'une vérification anonymisée. Un monitoring du comportement global d'un usager est interdit.

4. Effacement

Il faut distinguer l'effacement par le propriétaire du «compte» de l'effacement par l'opérateur.

Les organes publics ont le devoir d'effacer des informations ou des remarques problématiques sur le plan civil et/ou pénal. En outre, l'organe public est tenu d'effacer les données personnelles dans le respect de la législation cantonale.

Lorsqu'une requête d'effacement intervient auprès de l'opérateur, il n'y a pas de certitude que les informations ont été effacées définitivement. En règle générale, les informations continueront à être disponibles auprès de l'opérateur.

5. Protocole (Logfile)

Si des contenus illicites sont effacés par l'organe public, il faut pouvoir vérifier cet effacement (Logfile). La conservation des logfiles doit être compatible avec les réglementations cantonales.

6. La configuration des paramètres de «privacy» par les organes publics

Ci–dessous les paramètres pertinents sur le plan de la protection des données sont indiqués pour Facebook:

La configuration s'effectue en suivant les étapes suivantes:

Page adminstration -> „Modifier la page“ -> „Modifier les paramètres“

En outre les options suivantes peuvent être configurées:

a) Suppression de la possibilité de faire des commentaires, marquage et rédaction de messages:
„Autorisation de publier“, „Possibilité d’identification“ und „Messages“

b) Publication de commentaires devant être autorisée de façon préalable par l’organe public:
„Visibilité de la publication“ -> „Masquer les publications des autres sur le journal de ma Page“

c) Activation du filtre des termes utilisés, afin de bloquer des expressions vulgaires (notamment dans les commentaires):
„Filtre à injures“ –> „élevée“

Twitter n'offre pas de possibilité de changer des paramètres sur le plan de la protection des données.

7. Intégration d'un „plugin“ social

L'intégration de «plugins» sociaux est conforme à la protection des données, si elle a lieu avec suffisamment d'informations pour les utilisateurs et que la possibilité d’un choix suffisant leur est offert. Il faut prévenir une transmission non transparente et non voulue des données d'utilisateurs aux opérateurs, par exemple par «les boutons de recommandation à deux clics». Voir notamment:
http://www.edoeb.admin.ch/dokumentation/00153/00154/00167/index.html?lang=fr