Der Landesbeauftragte für den
Datenschutz und die
Informationsfreiheit
Baden-Württemberg

New Guideline on the use of social networks by public authorities issued by the State Commissioner for Data Protection and Freedom of Information of Baden-Württemberg

I. What's the point?

1. Social Networks - Supposedly Indispensable

Social networks such as Facebook, Twitter or Instagram have become an essential part of the professional and private communication behaviour of many citizens. Public entities also increasingly either use social networks, or plan to use social networks, for a multitude of reasons. For example, security authorities would like to incorporate social media into their administrations to give participants up-to-date information regarding meetings via Twitter. Municipalities, similarly, would like to point out their tourism offers via Facebook and respond to enquiries about such offers accordingly. Additionally, quite a few authorities utilize social networks as a tool for recruitment.

This guideline primarily focuses on the use of social networks for **public relations work** and for **distributing general administrative information** such as tasks, services, opening hours, contact data, contact persons, information on events, and moderation of discussions. This guideline will not focus on the provision or procurement of specific administrative services, as these aspects are, or will be, regulated by existing or future e-government laws.

2. Limits of Use by Public Entities

While citizens may use social networks at their discretion, **public entities** are subject to a **variety of legal obligations** not placed on the average citizen. Public entities also have an **exemplary function based on the rule of law**. Those in the data protection sector have repeatedly warned of this difference, but have (too) rarely been heard. The orientation aid now presented takes into account public entities' interest in using data as well as the data protection limits already placed on these entities.

3. This is Not About Messengers

The focus of this guideline is, therefore, on social networks that address the public. The use of so-called instant messaging services such as WhatsApp, Snapchat, and Facebook Messenger are subject to stricter conditions. This applies in particular in cases where there is a special protective and custodial relationship between the state and users – for example, in regards to issues concerning kindergartens or schools. Accordingly, these issues are not covered by this Guideline.

4. From a Legal Point of View ...

Social networks fall within the legal category of **telemedia** under Section 1 para. 1 of the German Telemedia Act (Telemediengesetz, TMG). However, the GDPR takes precedent in the area of Chapter 4 of the Telemedia Act and supersedes these TMG provisions. This is due to the delay in the legislative procedure of the ePrivacy Regulation, and the partially insufficient implementation of the old ePrivacy Directive into German law (see the DSK position statement "On the applicability of the TMG to non-public bodies from 25 May 2018" (in German)).

Despite offering information or communication services on one platform, social networks are often **multi-provider relationships**. Given this relationship, the user is faced not only with the respective **content provider**, who uses the platform to present itself, post or comment on content, but also the respective **platform operator**. This is particularly concerning given thatthis issue now also applies to public entities utilising social media platforms in the same manner. Not only does this make social networks difficult to understand from the user's perspective, this reality is often problematic from a legal point of view, particularly in regards to data protection responsibilities. **Fundamental issues remain unclarified**, even more so when dealing with non-European platform operators/providers.

Requirements such as competition law, public procurement law or special public law obligations of public authorities are not covered by this Guideline. Of course, other rules for public entities, such as the contractual connection to monopolists in the field of internet communication, must be observed here.

In any case, the Baden-Württemberg State Commissioner for Data Protection and Freedom of Information (Commissioner) sees a **joint responsibility under data protection law for public entities** that use social networks in the context of their tasks. This opinion is grounded in the fact that usage data is only created through the public bodies' use of social networks for offers, and the fact that such data is then processed by the respective platform operator. This responsibility gives rise to certain **legal obligations on the part of the public entities** (see II. for more information).

5. What exactly does that mean?

When social networks are used by public authorities, the following rule also applies: **no opportunity without boundaries**. State and local authorities are subject to a constitutional obligation of law and justice (rule of law principle), and have a special responsibility due to their exemplary role in society. This obligation extends to their use of social networks. In view of the obvious **deficits in compliance with data protection law** within a number of social networks, public entities should align their social network offers with the principles of **data minimisation** when processing usage data moving forward. Public entities should also **actively inform users** about the aforementioned risks to their personal data. In order to provide users with actual control over the usage of their data, there should be avenues in place that allow for user objection to data processing in social networks. However, if such means of objection are not possible through the social media platform, this lack should be compensated by informing and **educating** the users with regard to their usage of the social media platform. The public entity should also provide **alternative communication channels**, while informing the users that their usage of the social media platform is solely up to their discretion.

II. Requirements and Prerequisites

From the point of view of the Commissioner, public entities must take the following **four points** into account when using social networks: 1. a defined **usage concept**, 2. observation of the **obligations** under the Telemedia Act, 3. continuous supervision of social media usage/presence, and 4. the existence of **alternative information and communication channels**.

1. Clear Concept

a) Before using a social network, the public entity must provide a document describing the **purpose, nature, and extent** of their intended use of social networks. Moreover, the entity should provide the reasons for its decision in choosing the particular social network, in addition to the responsibilities for editorial/technical support, and the exercise of the rights of the persons concerned in accordance with Articles 15 et seq. of the General Data Protection Regulation. In doing so, the public entity must clarify the advantages (with regard to fulfilling its tasks) it hopes to gain from social media usage. It should also note the potential disadvantages that would result from ending such use.
   This concept forms the basis for the Commissioner's future audits.

b) The concept laid out above will **vary** depending on the public entity in question and the manner in which they utilise the social media platform. For example, within the framework of the public relations work of a ministry, different focal points may come into play when compared to those at play in a municipality or when recruiting young people. There may also

be differences in intended use depending on whether information is solely provided or whether the platform is also being used to communicate with citizens. In the latter case, careful handling, particularly of sensitive data, must be ensured.

c) Within this conceptual framework, a public entity must carry out an **assessment of the consequences of the planned processing operations** for the protection of personal data. As a rule, there is no obligation to notify the Commissioner regarding such assessment, but we, of course, would be happy to provide advice as to such endeavours.

d) The concept should be **evaluated** regularly so as to incorporate new information which may arise with further experience with social media. Such evaluation, should occur at least annually, and consider necessity and extent of the public agency's use of social media.

e) The developed concept and its evaluation should be made **generally accessible**, e.g. published on the Internet according to the model of Section 11 of the Baden-Württemberg State Freedom of Information Act (LIFG BW).

2. Design of the Network Offer: Observe Telemedia Act Obligations!

a) In accordance with Section 5 of the Telemedia Act, the public entity's social media offer must identify the **public entity** itself **as the provider** of the offer, as defined by the Telemedia Act. This information must be easily recognisable, directly accessible, and permanently available. This objective may be achieved by placing this information, referred to as "Imprint" or "Contact", as a separate item in the general navigation menu, allowing for access after a maximum of two steps.

b) The offer must have its **own privacy statement**, titled as such, and like the imprint, should be provided as a separate point in the navigation menu. In contrast to the imprint, however, the privacy statement should be available from each subpage of the offer. In addition, the privacy statement must reflect the tiered provider relationship described at the beginning of this guideline.

aa) For example, the privacy statement must inform users about the **processing of usage data by the platform operator** and about any transfer of data outside the European Union; a link must also be provided to the privacy statement of the platform operator. The statement should also contain a reference to problems related to compliance with data protection in regards to social networks, and the way in which processing of usage data may be limited (i.e. through data protection / privacy settings of the respective social network). If the social network used does not provide a permanently available privacy statement, users must be

regularly provided with a **reference** to the statement. Such provision should occur, depending on the frequency of new content, and at least on a monthly basis. This reference should also include a corresponding link to the text of the public entity's own privacy statement.

In addition, the public entity should inform and educate the registered users regarding their usage of the social media platform. The public entity should also **provide alternative information and communication channels**, e.g. the e-mail address of the authority or their website.

If the platform operator uses mechanisms that allow for recording a usage outside the respective social network (e.g. cookies, social plug-ins), the users must also be notified of such action, e.g. by means of a corresponding cookie banner or notice text. When using social plug-ins, the 2-click, or Shariff solution, must be used. If plug-ins are implemented in this manner, personal data will not be transmitted immediately upon website access, but only after activation of the plug-in through a separate click.
In this regard, the public entity has its **own duty to inform and check**.

bb) Moreover, if the public entity itself collects and processes personal data via the social network, the privacy statement must contain **information in accordance with Section 13 of the Telemedia Act** (type, scope, purpose of processing). In this regard, the provisions of Articles 44 et seq. of the GDPR must be observed (**data transfer abroad**). The public body bears joint responsibility for the social media network's collection of data in this manner. Accordingly, the public entity must inform visitors of its network page about such collection (for example, personal data is collected by the Social Network using cookies and used to make visitor statistics for the public body, the public entity bearing joint responsibility in this regard).

3. Continuous support of the public entity’s own offer

According to Section 7 para. 1 of the Telemedia Act, service providers are, in principle, only responsible for their own information made available for use. Providers are not responsible for third-party content and data processing. Consequently, a service provider is not obligated to check the contributions posted by users for possible legal infringements before publication. However, if the user has the opportunity to participate interactively (e.g. through comments) in the context of the offer by the public entity, and if the public entity becomes aware of an illegal act or information, it shall be liable pursuant to Section 10 of the Telemedia Act for failing to act and remove such information without undue delay. The public entity must, therefore, have its offer **supervised editorially by an appropriately trained person**.

Taking on responsibility also means taking regular (at least quarterly) **measures on the social media platform to notify users of the risks** associated with their use of the platform, and their right to informed decisions regarding use. For example, this may take the form of references to current data protection topics, contributions to data protection or to corresponding information offers.

4. Offer Alternatives

a) In principle, access to information from the public body must not depend on prior registration with a social network. The information provided on any social media platform must thus **always be available by alternative means** (e.g. the administration's website). Under no circumstances should a situation arise in which users are induced into usage of a social network because certain state or municipal information is available exclusively on the social media platform.

b) In particular, care should be taken to provide these alternative means of access when dealing with the **availability of interactive functions** (e.g. commenting, sharing, rating). If such functions are designed to allow for intensified dialogue with the public entity, an **alternative means of communication** outside the social network **must be offered** at all times (e.g. e-mail/telephone). Depending on the requirements, the public entity may use interactive functions, such as pointing out current events and danger situations, responding to comments and questions, and/or moderating communication, as long as processing and transfer of personal data are avoided to the extent possible and the use of alternative means is strongly encouraged.

III. Outlook

From the point of view of the Commissioner, this guideline provides a framework for action with which the expectations of users can be met with regard to participation by public entities in social networks. Despite the fact that some issues are still not regulated, this Guideline already allows recognised data protection standards to take effect.

European legislation on data protection, which has taken effect in May 2018, imposes far-reaching obligations on providers of social networks, particularly with regard to transparency and information for the individual. This has already led to adjustments for public bodies using social networks. The dynamic development in this field will cause need for further adjustment. The Commissioner monitors this development and will continue to offer advice and support in the future.