Austrian Federal Economic Chamber
Division Information and Consulting Wiedner
Hauptstraße 63 | A-1045 Wien
T +43 (0)5 90 900-3151
E ic@wko.at
W https://wko.at/ic

Advisor	*Direct Dialing*	*Date*
BSIC/ Iu Mag. Ursula Illibauer	-3151	08.01.2020

Public Consultation:
Guidelines Data Protection by Design and by Default

Dear Sir or Madame,

the Federal Division for Information and Consulting of the Austrian Economic Chamber would like to thank you for submitting the paper and we comment as follows:

The first pages contain very general statements, not so much about Privacy by Design and by Default (PDD), but about data security measures in general, state of the art, ect. From page 13 onwards there are more concrete examples of implementation or concrete requirements for PDDs mentioned. Nontheless we would recommend to implement more examples with a better view at economy and practical examples of implementation as well as concrete technical guidance.

1. Privacy by Design (Rz 1 – 38, in General):

In the context of PbD, appropriate measures must be implemented. Hereby the term „adequate“ is determined by the intended purpose of the processing and the effective reduction of risks to the rights and freedoms of data subjects. It is appreciated that no „over the top“ measures are recommended, but measures such as simple employee trainings. Another important point would be an explicit reference to the fact that the „state of the art“ also takes into account the needs (and capacities) of SMEs (similar to Art 42 (1) GDPR).

2. Enforcement and ensurement of the principles of Art 5 GDPR

- **Transparency**: „Key designs" and „key default elements" would involve enormous effort and must therefore be rejected. This applies in particular to the provision of contextual information at the relevant time and in an appropriate (different?) manner. This would lead to a fragmentation of the data protection information that must be avoided. Individual pieces of information via small snippets or pop-ups could never represent all the information and would therefore normally be incomplete and thus misleading. Furthermore, it should be ascertained that a link to the website´s privacy policy in general is sufficient (therefore also in the offline context).

- **Lawfulness**: Bank lending is given as an example. In this case, the bank acts as a bad example when granting a loan, since it uses not only the personal details the bank directly acquires from the data subject but also information from the tax authority (how is a bank able to get this information??). For the latter, however, the bank needs the consent of the potential customer, as this is no longer covered by the contract. This is incorrect, as it can be argued either with the necessity of the contract or at least with a legitimate interest in regard to credit default calculation. The current wording could also cover every publicly available information, such as information from the commercial register court which cannot be the intention of the EDPB.

- **Fairness**: The term „consumer-choice“ has been chosen incorrectly, as it clearly identifies a data subject who is not only a consumer but a SME as well. The list (point 65) is hardly helpful, rather causes confusion. As an example, search engines are mentioned, which function by processing personal data and offer a „free choice of the consumer" in search results. The meaning and the intention of the example is unclear. The second example covers a streaming service which offers additional customer service for an extra charge. In this case, however, "customer service" should not mean preferential treatment in terms of data subject rights acc to GDPR. As this is common sense, the example does not add value for interpretation of the GDPR.

- **Purpose Limitation**: The example contains an Costumer Relationship Management System. The technology provider shall offer these CRM in such a way that the person responsible (controller or processor) can already assign the different purposes for the data processing. It is crucial that this point will be deleted. The responsibility of providers, who are neither controller nor processor, is already covered by general consumer and civil law and has no place in the system of the GDPR. In this sense, the "recommendation" on page 26 that „technology providers" should play an active role in fulfilling the obligations under Art 25 must also be rejected. It is the responsibility of those responsible for using the software. One (a technology provider) can never predict how the software is used by a controller or processor.

- **Data minimization**: An online shop should, for example, only request those data that are „actually necessary for the fulfillment of the contract“ (f.e. while using a default input-system in an online form). In the EDPB´s view, neither the date of birth nor a telephone number would be necessary data. This is not legitimate. Enforcement of a contract and payment must be guaranteed, in which the date of birth can play a significant role. The date of birth may also be necessary to determine the age of a data subject (see Article 8 GDPR) or for preventation of fraud.
  In statistical surveys and analyses, pseudonymisation and anonymisation should also be included at the earliest stages. This is highly impractical. These surveys and analysis usually deal with the unambiguous allocation and merging of duplicates (e.g. the date of birth in combination with name and address is a unique identifier). This not only helps to combat fraud, but also ensures that the data is processed correctly.

- **Storage limitations**: „Make sure that it is not possible to recover deleted data“ is not state of the art. Better wording must be chosen that takes into account technical possibilities and proportionality.

- **Integrity and confidentiality**: In this example, transmission of patient files must be protected in a very special way. However, the example reaches very far, a whole range of measures is prescribed which must be ensured before the transfer can take place (point 80, example). These measures are highly impractical and therefore must take into account that most technical solutions are not there yet.

We support the statement that certifications according to Art 42 GDPR may constitute appropriate measures. It would be essential to give special consideration to SMEs (Art 41 (1)).

Kind Regards,

Division Information and Consulting
Wiedner Hauptstraße 63
A-1045 Wien
+43 (0)5 90 900-3151
ic@wko.at
https://wko.at/ic