

**comments on the "Guidelines 01/2022 on data  
subject rights - Right of access"**

We appreciate the clarifications and explanations offered by this guideline. Especially the examples will simplify the working process of persons involved in the handling of data subject's requests. However, some points could be misunderstood, are not interpreted easily and correctly or should be avoided at all.

#### **Paragraph 40**

*... sending a USB-stick by (registered) letter post to the data subject*

This passage describes the application of what we consider to be, firstly, an outdated and also not state-of-the-art IT security requirement to send unencrypted USB sticks, even if the mailing is registered. It should be clarified when end-to-end encryption is necessary at all. There are no recommendations on this yet. The recommendation should at least be reformulated to the effect that secure, electronic data exchange platforms should be used as a matter of preference.

#### **Paragraph 57**

*The EDPB considers as good practice for the controllers to confirm receipt of requests in writing, for example by sending e-mails (or information by post, if applicable) to the requesting persons confirming that their requests have been received and that the one month period runs from day X to day Y....*

Good practice or obligation?

#### **Paragraph 74**

*Taking into account the fact, that many organisations (e.g. hotels, banks, car rentals) request copies of their clients' ID card, it should generally not be considered an appropriate way of authentication.*

If the controller has other means of verification, those should have been used. Only then, the controller has to ask for more.

#### **Paragraph 76**

*To follow the principle of data minimisation the controller should inform the data subject about the information that is not needed and about the possibility to blacken or hide those parts of the ID document.*

We suggest formulating positively: ... the information that is needed and about the possibility....

### Paragraph 89

*... There is, however, no obligation for the controller to provide the data under Art. 15 directly to the portal. ...*

The controller can decide the way of electronic confirmation. The data subject can only decide whether post or electronic.

### Paragraph 89

*...If the controller, for example, establishes that the security measures are insufficient, it would be deemed appropriate to use another way for the disclosure of data to the data subject. Under such circumstances, ...*

This sentence implies the obligation on the controller to assess the portal's security measures. Why should controllers be forced to assess portals in different jurisdictions? E.g. mine portal  
→ Delete this sentence and the following three words without replacement

### Paragraph 104

*...messages that data subjects have sent to others in the form of interpersonal messages and deleted themselves from their device, that are still available to the service provider, may fall under the right of access.*

With an Art 15 request, you get your restore function for free?

### Paragraph 115

*...The controller should therefore generally name the actual recipients unless it would only be possible to indicate the category of recipients. ...*

In contrast to the cited "Guidelines on transparency - endorsed by the EDPB, p. 37 (Annex)" namely "If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients." the guideline leaves no option to the controller. If a controller has to disclose all processors to a data subject, this infringes "trade secrets" and is not useful of a deeper understanding of the processing. See also # 166 and # 168: "...trade secrets ....". and the employed processors are to a certain extent a trade secret.

### Parapgraph 138

What is the sense in providing log files (with or without explanation)? The examples are very clear, but the wording of the text is contradictory. Especially following the example you could get the impression that for all self-service offers, the controller has to provide log-files and not just a compilation → in contradiction to # 150.

### Paragraph 139

See comment to # 138

### Paragraph 144

See comment to # 138

### Paragraph 147

*What could be considered as a commonly used electronic form should be based upon the reasonable expectations of the data subjects ...*

See comment to # 89 – especially seen from the point of view that for many data subjects it may seem reasonable to be answered via WhatsApp or Facebook.

### Paragraph 148

*... stored on an electronic storage device, such as CD or USB.*

Even if the letter post is registered it doesn't prevent the USB-Stick from getting lost – if it is not encrypted with a password, this results in a (possibly) severe data breach. Has everybody nowadays got a CD-reader or USB-Port?

### Paragraph 171

*This means, for example, where the limitation applies, that information concerning others has to be rendered illegible as far as possible instead of rejecting to provide a copy of the personal data*

This passage is about the fact that if there are parts in a data disclosure that could have negative effects on the rights and freedoms of other persons, these parts should be left out or rendered illegible. "leaving out or rendering illegible those parts". In practice, this would mean that such documents or, for example, emails, correspondences must be blacked out or electronically cut out. We see this clarification as imposing a very high additional burden on companies. The passage should either be deleted or reworded to the effect that such documents do not have to be provided.

#### Enquiry note

Dipl.-Ing. Ursula Tauschek  
Head of Networks

Österreichs E-Wirtschaft  
Brahmsplatz 3, A-1040 Wien  
phone: +43 1 50198 223  
e-mail: [u.tauschek@oesterreichsenergie.at](mailto:u.tauschek@oesterreichsenergie.at)  
[www.oesterreichsenergie.at](http://www.oesterreichsenergie.at)