March 2022

ETNO response to EDPB Guidelines 01/2022 on data subject rights - Right of access

ETNO welcomes the opportunity to comment on the draft Guidelines 01/2022. We highly value article 8 of the EU Charter of Fundamental Rights. The right of access for data subjects has been implemented by the members we represent since Directive 95/46/EC came into force. The members have looked closely at Article 15 GDPR and the corresponding considerations 63 and 64 when the GDPR came into force to determine whether any changes were necessary. The right of access has been actively exercised by data subjects without major problems or complaints for many years.

However, we are of the opinion that the draft Guidelines as published by the EDPB have unintended effects for users of telecom services and go beyond the intention of the EU legislator, especially as expressed in recitals 63 and 64 of the GDPR.

Furthermore, ETNO supports the EDPB's aim to explain their Guidelines in a simple manner and with practical examples. However, the Guidelines should also reflect the complexity of the IT solutions landscape in the industry, where there might be hundreds of IT solutions from different technological cycles. Executing the right of access in such an environment requires a skillset with different solutions and a holistic management of the access process, rather than considering individual systems separately.

Concept of personal data and scope of right of access

The case law referenced by the EDBP gives a broad definition to the scope of the concept of personal data. Nevertheless, the common denominator in the mentioned case law[1] and in the case law that is mentioned in the Nowak case[2] is that the data is objectively useful to the data subject. If the scope were in fact to include all observed raw data in IT systems and non-IT filing systems, as proposed by the EDPB, telecom traffic data would also be included. The broadening of the scope of the right of access for a data subject (the subscriber or a user of a telecom service, if subscriber and user are separate individuals) to these raw data would lead to the following undesirable effects:

1. For the sake of protecting the callers, certain numbers are deliberately not included on the invoice, for instance calls made to organisations where abused children can get advice for help. This

[1] CJEU, C-434/16, Nowak, paragraph 56.

[2] Rijkeboer, C-553/07, EU:C:2009:293, paragraph 59.

information would be available on the raw data (call detail records) and presenting this information could have serious negative impact on the privacy and possible physical wellbeing of other data subjects. It is important to remember that the same telecom services are not only used by the subscriber, but also by other data subjects (e.g., the subscriber's phone or messaging interlocutor). These persons deserve privacy protection as well. The right of access afforded to the data subject should be always balanced against the fundamental rights of other people that could be affected by the exercise of such access right.

2. A lot of data processing activities within telecom companies are based on standards, for instance from the 3rd Generation Partnership Project (3GPP). This enables subscribers of telecom provider A to communicate with subscribers of telecom provider B. A lot of this processing is based on standards such as the 3GPP TS 32.298. The complexity of this processing is so great that the related data processing is not realistically explainable to laymen. Furthermore, the data processed would not provide the data subject with any real insight into the data processing that has taken place. Our position is that the overview of the processing of personal data is sufficiently provided by means of the itemised invoice that the subscriber (or user, if separate individuals) receives. The itemised invoice shows for instance information about the numbers called, the duration and the cost of each call or rented movies.

3. The use of telecom services creates a sheer amount of raw technical data: every call or download will create an item. These items are stored for billing purposes for at least 6 months. This also applies to television services (although a different retention period applies), e.g., data processed by telcos include which programmes are watched, channel changes, when the subscriber pauses or fast-forwards the video stream. This large amount of technical data does not provide meaningful information for the subscriber/data subject about the processing that takes place.

Since this technical data is already heavily regulated by national legislation in the different member states as part of the broader traffic data based on the e-Privacy Directive, this data is not subject to the GDPR. This would remain the case with the upcoming e-Privacy Regulation. Therefore, this technical data is excluded from the scope of the right of access for the above mentioned reasons[3].

ETNO has long called for consistency of the various horizontal and sectoral regulations protecting the data and privacy of European individuals, in order to provide legal clarity to both data subjects and data controllers. This need for coherence is all the more crucial as EU decision-makers are set to introduce further measures affecting the right of data access in additional pieces of law, such as the Digital Markets Act and the Data Act.

[3] As an example, national laws based on e-Privacy Directive may regulate what can be displayed on the itemised invoice when subscriber and user are not the same person. These rules override the Right of Access under the GDPR.

Figure 1: Example of log record generated on a Set-top box (STB)

Log record type	Example	Explanation
LALE_Event_ID	DTV-CH	Log event type, DTV-CHG is a "Channel Change"event, but there are also other events like "Power On" and "Power Off"
LALE_MAC_Address	0001f880e2384363a9a63802fc9e5437	By default a meaningless HASH-Key, only filled with a real MAC-Address if the customer has given an explicit Opt-In
LALE_IP_Address		Always empty by default, only filled if the customer has given an explicit Opt-In
LALE_Subscriber_ID		Always empty by default, only filled if the customer has given an explicit Opt-In
LALE_Viewer_ID		Always empty
LALE_Event_DateTime	2022-02-21 12:14:06.037	Date and time of the event
LALE_Event_Duration	212	Calculated Lead Time of the Event (after lapse)
LALE_Event_CallLetter	NPO3	Channel code
LALE_AVR_Spec_Version	NULL	Software version of the STB
LALE_STB_Name	NONE	Name of the STB if the customer enters this themself, examples are: "Living room" or "STB-1"
LALE_InFo_Field_01	EP000877660033	Optional Data field in relation to the event, with a channel change or programme change, here is the technical reference to the programme
LALE_InFo_Field_02	NULL	Optional Data field in relation to the event
LALE_InFo_Field_03	NULL	Optional Data field in relation to the event
LALE_InFo_Field_04	NULL	Optional Data field in relation to the event
LALE_InFo_Field_05	HD	Optional Data field in relation to the event, with a channel change or programme change, here is the technical reference to the resolution of the broadcast (SD, HD,..)
LALE_InFo_Field_06	NULL	Optional Data field in relation to the event
LALE_InFo_Field_07	Next Program Starts	Optional Data field in relation to the event, in the case of a channel change or programme change, here is possibly the description of the reason for this channel or programme change
LALE_InFo_Field_08	NULL	Optional Data field in relation to the event
LALE_InFo_Field_09	NULL	Optional Data field in relation to the event

Normally an STB hooks up to a Multicast stream. The default setting is that the STB generates a completely anonymous log record, where the MAC address is encrypted (Hash) using a generated key on the STB, which only the STB itself knows. This means that the provider cannot send log records to customers, because it does not know who the customer is. Only if the customer has given an explicit Opt-In does the log record contain the technical ID (TAN) of the customer.

Information to the data subject

According to paragraph 139 of the Guidelines, information provided to the data subject must be 'intelligible', i.e. it should be understood by the intended audience. This shall also and in particular apply e.g. to raw data, codes, activity history etc. To meet this requirement, the controller shall take the necessary measures to ensure that the data subject understands the data, for example by providing an explanatory document that translates the raw format into a user-friendly form such as explained abbreviations, acronyms etc. According to the Guidelines, this means that copies must not only be provided to the data subject in accordance with Art. 15(3) GDPR, but that the content must also be explained.

However, Art. 15(3) GDPR only provides for the right to receive a copy of the personal data that has been processed. The obligation to provide information in a transparent, comprehensible and easily accessible form, using clear and plain language, only applies to the information provided pursuant to Art. 15(1). An obligation to prepare the content of the copies, as ostensibly demanded by the EDPB, results neither from Art. 12(1) GDPR nor from Art. 15(3) GDPR.

Personal identification

Another issue we would like to raise is with paragraph 73 regarding the inadequacy of asking for a copy of ID as a part of an authentication process. The EDPB states this use should be considered inappropriate. ETNO maintains the principle that excessive processing must always be prevented and that less intrusive alternatives should always be preferred over more intrusive methods if the same result can be achieved.

On the one hand, the identity of the data subject must be reliably established; on the other hand, this must not be such an obstacle that impairs the data subject's right to freely interact with an organisation. For that reason, it is always wise to examine the processing of personal data, such as when invoking GDPR rights.

ETNO members wish – and are also legally obliged – to reliably establish the identity of the data subject when invoking his/her rights, but also to prevent information from being shared with unauthorised third parties with all the associated consequences. ETNO fulfils this obligation with an unambiguous process in which individuals involved can confirm their identity by submitting a protected copy of ID (i.e., without a photo and without national identification number).

This standard working method guarantees proper identification without prejudice to the right of data subjects to contact an organization freely and without excessive processing taking place in view of the mitigating measures mentioned above. This approach is also in line with the decision of the Dutch Council of State of 9 December 2020 (ECLI:NL:RVS:2020:2833), in which the Council does not consider the principle that a copy of an identity document is required with a request for access to be unreasonable.

Personal data that is being processed

In paragraph 108, the EDPB equates data in back-up systems with data in live systems. Likening back-up systems and live systems would mean that, by default, a back-up system must always be searched, regardless of whether the search in a live system has led to a result.

Notwithstanding of the disproportionate effort involved, this requirement not only does not serve the rights and freedoms of the data subjects, but also contradicts the principles of data minimisation and storage limitation. If, for example, data has already been deleted from the live system, it is inaccessible to all employees and is also removed from the back-up system during the next deletion cycle. This access restriction on data that has actually been deleted from the live system would no longer apply if back-up systems also had to be checked regularly.

The same applies in principle to the EDPB's requirement to provide information about data that is only stored due to a legal obligation, as per paragraph 107. This data is subject to very strict access restrictions and is in principle not accessible. This strict access restriction as an expression of the principles of data minimisation and storage limitation would be breached if service employees regularly had to search this data also to respond to information requests.

About ETNO

ETNO (European Telecommunications Network Operators' Association) represents Europe's telecommunications network operators and is the principal policy group for European e-communications network operators. ETNO's primary purpose is to promote a positive policy environment allowing the EU telecommunications sector to deliver best quality services to consumers and businesses.

For questions and clarifications regarding this paper, please contact Paolo Grassia, (grassia@etno.eu) Director of Public Policy at ETNO.