53.

CONFEDERATION OF INDUSTRY
OF THE CZECH REPUBLIC

PRAGUE, 30 JANUARY 2017

Position to the material of Article 29 Working Party: GDPR Interpretation Guidelines in the field of Data Portability, Data Protection Officers and Identification of the Lead Supervisory Authority

INTRODUCTION

The issue of personal data protection in the digital environment is one of the priorities of the Confederation of Industry of the Czech Republic (Svaz průmyslu a dopravy ČR – further referred as "SP CR"): it is among the priorities of the Expert Team for the Digital Economy, which roofs also a specialised Working Group on Data Protection. SP CR is also an active member of the Working Group of the Office of the Czech Government for the Legislation in the field of Data Protection. Mapping the state of preparation of the enterprises in the Czech Republic to introduce the new obligations raising from the new EU General Data Protection Regulation (Regulation of the European Parliament and of the Council (EU) 2016/679 of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data – further referred as „GDPR"), SPCR has also realized a research among the Czech entrepreneurs in the end of 2016 and, for the 1st half of 2017, it prepares a series of regional discussion forums with entrepreneurs.

Following the publication of the interpretation guidelines to GDPR approved at the meeting of the Article 29 Working Party as an advisory body of the European Commission in the field of personal data protection on 13th December 2016, SP CR would like to apply now the following comments to the published documents:

1. GUIDELINES CONCERNING THE RIGHT TO DATA PORTABILITY

Introductory Remarks of SP CR

- *The rights concerning the data portability are being interpreted in a very wide sense,*
- *The main philosophy of the Art29 WG is to renew the balance between the data subject and the controller, however, according to our opinion, this new setting up of the balance significantly disadvantages the controllers and it is in question, if this is supportable and, in the practice, performable,*
- *The ideological explications about that the portability will support the innovations should maybe serve as an apology for the requirements leading to such a wide scope of this obligation will mean for the enterprises. However, in the regards of the contents of the guidelines, it is not relevant at all and unnecessarily widens the content of the guidelines.*

PHONE (+420) 225 279 111 | E-MAIL SPCR@SPCR.CZ
WEB WWW.SPCR.CZ | ADDRESS FREYOVA 948/11, 190 00 PRAGUE 9, CZECH REPUBLIC
THE CONFEDERATION OF INDUSTRY OF THE CZECH REPUBLIC HAVE SIGNED UP TO THE EU TRANSPARENCY REGISTER AND THE ASSOCIATED CODE OF CONDUCT. REGISTER IDENTIFICATION NUMBER: 28582051412921.
MEMBER OF BUSINESSEUROPE

Comment of the Ministry of Interior of the Czech Republic (further referred as "MVCR"): It is necessary to distinguish, what is the recommendation and an example of a good practice, that puts in place WP29 and what is already the guiding principle or obligatory interpretation, which will lead to the decision making of the supervisory bodies and imposing the penalties. The present guidelines do not distinguish with enough clarity.

Specific Comments

Main Principles of the Data Portability

Right to Access, Get and Transmit the Personal Data (page 4)

- The term "data provided by the data subject" is being interpreted in a very wide sense – not only as data directly provided by the data subject, but also as the data provided indirectly, i.e. within the behaviour monitoring of a data subject and within the service provided (which means data provided, although indirectly, in every cases by the data subject itself). The outcome of analysis of such a data are however secondary data created by the controller.

- The only data that are not being transmitted are the anonymized data and the data derived by the data controller on the basis of the data provided by the subject ("inferred data and derived data", i.e. scoring on the basis of the provided health data).

- The right to portability is a "consumer oriented right", it has to promote the multiple choice of the user, possibility to control the data and consumer rights.

Examples

  - *Ex. 1 Data subject wants to gain his present playlist from the service providing music streaming so that he could discover to which songs does he listen most frequently and decide about which of them will he buy at another platform which he migrates to.*

  - *Ex. 2 Data subject keens on gaining mailing list from his own emailing application to set up a guest list.*

  - *Ex. 3 Data subject wants to gain information about his purchases using his customer's card for getting information about his own preferences.*

Comments of SPCR:

- *Widening of the scope of the provision to "observed data" in the general sense (i.e. when controlling the movements of the employees or monitoring the behaviour of the website users) is too wide and is not in line with the text of GDPR.*

- *Under all circumstances, the primary question should be if the data subject (consumer) has the legitimate interest to transfer the data to another controller. The data transfer should be realized only in such a case, where such an interest to transmit the data exists. Because of this, the right to portability should under no circumstances be applied to the data of the employees provided within a labour contract, as the legitimate interest could not be given – inter alia because this would interfere the interests of the original employer to protect his confidential data.*

WP 29:

- Recommend to categorize the collected data, document them and insert them into an automated function "portability",
- Considers to the controllers to use a function "data portability" (page 5), which means to offer not only possibility to download the processed data, but also to enable the data transfer using the online access providing filters through an Application Programming Interface (API) which would decrease the contents of the transmitted data and offer easier transfer,
- Recommends to the controllers to explicate clearly to what types of data this right applies and, therefore, could be required from the side of data subjects. Consequently, it is recommended so that the controllers would always inform about the possibility of the transfer before deleting the account,
- Prevents that the data subjects can also wish to use for the personal data storage a credible third party so that it would keep their data and grant to the data controllers the permission to access this data,
- In the cases when the data are being collected online and connected with pseudonyms and unique identificators, the controller could implement the appropriate processes enabling to the subjects to raise the requirement to transfer his personal data. In any case, the controller has to introduce an authentifying method for verifying the identity of the data subject,
- Recommends to the controllers to provide, within their informational duties, the data subjects also with the explication among the right to data portability and right to access the data,
- According to our opinion, it derives without a substantive foundation and in a certain manner arbitrarily that the term "personal data provided by the data subject" should be interpreted widely (page 8) and it classifies under this term not only data provided by the data subject, but also "data created by the own activity of a controller". Such a wide term is, within the WP29 interpretation, being widened also to the data that are the outcome of the activities of the controller, which means the data that have been created as a result of a service provided by the controller.

Comment of SPCR: This will require administrative, organisational and technological provisions: the revision of the current data architecture of the organisation of the controller, calculations of the new solutions, investments into redesign etc. Furthermore, the widening interpretation of WP29 further applies the right to portability not only to the personal data of the data subject asking for the transfer of his personal data, but widens this right also to the personal data of third data subjects, which remarkably affects their rights. This approach is inapplicable in a legal state.

Comment of the Office for the Personal Data Protection (further referred as "UOOU"): The interpretation is problematic – the guidelines are drafted in too wide range. It is not in place to use the term "sent/provided by the third party" but "delivered and accepted by the data subject".

Controllership – page 6

- New data controller shall ensure that the obtained data will be kept only in the scope needed for the further processing.

  Example: If the data subject will be willing so, the original controller will provide the information about the transactions at the bank account of a data subject to another controller expected to help

him with his personal finances. The new controller does not necessarily need all the details of the transactions and, therefore, he uses only the needed information.

- The personal data not needed for the new processing should be deleted.

Data portability vs. other rights of the data subjects

- The right to portability should not limit the rights and freedoms of the other persons,
- If the new data controller wants to process all the set of data including the personal data of more subjects, and if he has obtained this data on the basis of the right to portability to one of the subjects, he has to gain a consent from all the other data subjects on the basis of Article 6 (1),
- Right to portability does not automatically imply the deletion of the data from the systems of the original controller and does not interfere the original retention delay related to the transmitted data. The data subject can use the right to portability during all the time when his data are being processed by a controller,
- In the case if set of data contains data of a group of data subjects (i.e. telephone calls), the original controller should be able to execute the right to portability, but the new controller cannot under no circumstances use the gained third parties' data to the new processing and limit their rights and freedoms. For example if data subject transfers his contact list to the new e-mail account, the new controller could not mine the list for his marketing reasons,
- The portability requirement can be subject of a payment in the case if proved that the requirement is unreasonably repetitive. WP29 informs that the refusal of information could be justifiable only in minimum of cases. It alleges that, within the information society, the repetitive requirements can represent an overwhelming burden only with a very low probability. The overall costs of the processing of portability requirements should not affect the level of the burden,
- Time limit to fulfil the portability requirement: the controller will handle the requirement without an unreasonable delay, until one month from raising of the requirement at the latest. In the case of complicated requirement, the delay could be prolonged up to three months and the subject should be informed about the reason.

  Comment of SPCR: WP29 does not precise, what should be understood by the term "complicated requirements".

Comments of SPCR: The new controller (controllership, portability vs. other rights) will have to exclude data not relevant for the processing – does this imply that he will need to elaborate an analysis? Alternatively to ensure the new consents from data subjects? How this could be realized in a practice?

Intellectual Property and the Safety of the Transferred Data

- Although the right to intellectual property and the trade secrets, as well as the copyright have to be prevented from potential risk of abuse or affection, the protection of such a rights cannot serve as a reason for a refusal to answer the portability request. It is up on the controller to perform the transfer by such a mean that will not affect the trade secrets or intellectual property rights.
- As the data subject can fail in the field of security of the data transfer, the data controller is responsible to take up all the necessary provisions to ensure that the data are securely transferred

(i.e. encryption) to the right destination (using the additional verification) an help the data subject to secure the data transfer.

- WP29 also prevents that the data controller should, in the connection with the data transfer, inform the data subject that his personal data storage could not to provide enough safety to the transferred personal data.

Comment of SPCR: Here we can observe the clearly unbalanced bias of forces to the detrimentally to the data controllers – they are not protected against the trade secrets or copyright abuse and they are obliged to carry the duty of securing the data transfer with the reasoning that "the data subject could fail". There are no compensations or means to support the enterprises. If their rights will be affected, only their own administrative and financial burden will raise. WP29 visibly presumes that, in the field of security of data transfers, the controllers will actively involve it and in some cases also ensure it themselves instead of the data subjects.

2. GUIDELINES CONCERNING THE DATA PROTECTION OFFICERS - DPOs

Obligation to designate a Data Protection Officer (further referred as "DPO")

- Unless it is obvious that an organisation is not required to designate a DPO, the WP29 recommends that controllers and processors document the internal analysis carried out to determinate whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly. It could be presumed that, in the opposite case, the controller will be considered as not acting enough carefully in the sense of GDPR,
- When an organisation designates a DPO on a voluntary basis, the same requirements under GDPR will apply,
- WP29 recommends, as a good practice, that private organisations carrying out public tasks (i.e. in the field of water supplies, energy, transport infrastructure, public broadcasting, housing services, supervisory bodies within the professional associations etc.) would ensure their tasks via designating a DPO,
  Comment of UOOU: The interpretation out of the scope of the Regulation is not possible – there will be always evaluated if the need to designate a DPO is given, disregarding the recommended fields of doing business.
- Other examples of organisations that will have to ensure a designation of a DPO – telecommunications networks and services, e-mail marketing, profiling and risk evaluation (loans, insurance, prevention of fraud and money laundering), work with person locations (mobile applications), fidelity programmes, behavioural advertisements, lifestyle and health monitoring using the mobile devices, TV broadcasting with a limited circles, connected devices as smart meters, smart automobiles, devices for home automation etc.,
- WP29 does not define what to understand by an "large scale of data processing" or does not specify if this category should be interpreted in a national or international context,
- WP29 alleges that, also in the case if the controller meets the criteria for designation of a DPO and a processor is not obliged to do so, it is, within a good practice performing, good to designate a DPO also for a processor,
- DPO of a processor should supervise not only the activities carried out in the connection with the processor's services, but also those where he is a processor himself (HR, IT, logistics).

Comment of SPCR: Wide range of organisations obliged to ensure the DPO role performance is being further widened by WP29 expectations of the good practice and ensuring the DPO designation also at those organisations, where the obligation to appoint a DPO is not laid down in the Regulation. In this scale, it will be very complicated to ensure an appropriate number of qualified DPOs and, regarding their deficit, it will be also more financially requiring.

Comment of MVCR: What does it, according to the guidelines (page 7) mean "large scale" of the data processing? The guidelines do not bring enough clarity, on the opposite it further complicates the interpretation.

Comment of UOOU: The simple fact that the controller offers the possibility of processing data, does not mean, that he really performs it – therefore, it is necessary to evaluate the real scope of data processing according to the actual situation. It is also necessary to apply the quantitative criteria.

Easy accessibility of a DPO

- According to Articla 37 (3), a single DPO may be designated for several public authorities or bodies, taking accound of their organisational structure and size given the fact that he is easily accessible from each of these organisations – therefore, he must be, according to WP29, able to effectively communicate with the data subjects and cooperate with the supervisory bodies. The communication must take place in the language used by the supervisory authorities and data subjects concerned.

Comment of SPCR: This means that the possibility given by Art 37 (3) is only an illusion? We will need a further explication concerning the accessibility and language equipment of the DPO.

Comment of UOOU: On a working line, it would be made possible to communicate in the "basic EU languages" (EN, FR, DE), but the official communication has to take place exclusively in CS. "Easy accessibility" means the standard accessibility in a working/business hours.

- When appropriate, the DPO has to be accessible also via hot-lines or dedicated contact form addressed to the DPO on the organisation's website.

Comment of SPCR: These duties go again outside the scope of GDPR and widen the duties posed on controllers/processors, although this is only an interpretation of GDRP. Does this mean that the organisations have to ensure a hotline or secure communications channel? What technological and financial impact will this have?

Professional qualities of a DPO

- WP29 implies that the knowledge of the business sector and of the organisation of the controller is useful for a DPO.

SPCR comment: However, we consider this knowledge as a principal one for good performance of the DPO role – it is necessary to avoid the situation that DPOs will be mainly lawyers or external consultants.

UOOU comment: This implication is very unclear.

Necessary resources for the performance of a DPO role

- If a DPO executes also other functions, it is necessary to establish a percentage of time for the DPO and avoid the conflict of interests,
- Adequate financial resources, infrastructure (premises, facilities, equipment) and staff for performing the function of a DPO,
- Access to other services as HR, IT, legal, security etc. So that DPO can receive essential support, input and information from those other services,
- Continuous training, presence at the trainings dedicated to data protection issues, workshops, data privacy fora, etc.
- Given the size and structure of the organisations it may be necessary to set up a DPO team,
- DPO has to be independent and should not be subject of any direct or indirect penalisation in the connection of performance of his duties (prevention from career advancement, denial from benefits etc.). The service contracts with DPOs (labour as well as the service ones) have to be as stable as possible,
- DPO is not personally responsible for the performance of its function and for the sanctions imposed to the controller, as it is only controller, who is responsible for the compliance with GDPR.

SPCR comment: This all implies significant financial and organisational requirements to ensure the function, it will be very complicated to engage more than one DPO in one organisation regarding the great lack of the appropriate persons in the market and further limitations raising from a possible conflict of interests. The wide range of the protection of the DPO independence creates almost a position of a "upper-employee". The WP29 implies doubts if it is possible to terminate the internal labour contract with DPO, i.e. for inappropriate working results.

UOOU comment: Situation is very unclear and misleading, it is necessary to handle the solutions in a practice way. "Group of DPOs" – it is unclear, it is necessary to appoint a "leading DPO" who will be the person dedicated to communicate internally with the organisation and externally with the supervisory authority.

Conflict of interests

WP29 recommends so that each organisation:

- Makes an internal evaluation, which positions are in fact incompatible with the DPO functions,
- Draws up internal rules to this effect in order to avoid conflicts of interests including a more general explanation about conflicts of interests,
- Declares that their DPO has no conflict of interests,
- Elaborates safeguards in the internal rules of the organisations and ensures that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests.

SPCR comment: Other administrative and financial requirements for elaborating an internal assessment and rules. I.e. it is necessary to clarify, if a cybersecurity specialist will be in a position to carry out the duties of a DPO? Possible accumulation of activities (and working tasks) of individual inhouse DPOs would be certainly desirable and, in the case of SMEs, even necessary.

UOOU comment: It is necessary to take into account an individual situation and internal culture of each the enterprise – it is necessary to evaluate it and, on the opposite, the accumulation of functions in the situations where no conflict of interests exists is desirable. The guidelines do not in any case establish

concrete examples of conflicts of interests, it is necessary to evaluate in merito and individually. Nevertheless, the evaluation of the existence of the conflict of interests has to be performed independently.

Role of the DPO in the process of Data Protection Impact Assessment - DPIA

- From the explication of WP29, it is clear that the DPO should have a consultative role in the process of DPIA, however, it is not his task to perform it himself.

SPCR comment: The businesses will therefore need to ensure this externally or internally. This means other requirements imposed on the human or financial resources.

UOOU comment: DPIA has to be performed in a properly independent way – no matter if internally or externally.

Role of the DPO in the process of record-keeping of operations carried out by the controller

- This activity is a primary task of a controller or a processor, not the DPO. DPO should create the inventories and hold a register of processing operations based on information provided to them by the various departments in the organisation (IT, HR, legal etc.). The documentation of the operations is, in the same time, also the instrument for the supervisory authorities for the evaluation of the compliance with the Regulation.

SPCR comment: What does it mean "creation and holding the registers for the enterprises? What administrative and financial requirements will this represent? How this could be ensured in a technological way?

UOOU comment: It is necessary to establish a single storage or single access to all the information and operations of the data processing within the various systems used by organisation.

3. GUIDELINES CONCERNING THE IDENTIFICATION OF A LEAD SUPERVISORY AUTHORITY

- The identification of the lead supervisory authority is necessary in the cases, where a controller or processor is carrying out the cross-border processing of personal data. This mechanism is euphemistically entitled "One-Stop-Shop".
- Lead supervisory body is in the state where the organisation has its EU headquarters and where the decisions concerning the data processing are taken. If the controller is in one Member State and a processor in another one, then the lead supervisory authority is in the Member State, where the seat of the controller is placed. It is presumed the hierarchical structure of the decision-making of the international companies.
- However, if the decision making concerning the data processing is taken in more of the Member States (i.e. a bank is seated in one State but has its Insurance Division in another one and Loan Division in the third one), it will be obliged to cooperate with the supervisory authorities in all the relevant States.
- If the organisation does not have an EU headquarters and operates in the EU through its representation, the possibility to identify the lead supervisory body does not apply to it and it will be obliged to cooperate with all the supervisory authorities in the relevant Member States.
- The process of identification, where the decision making process concerning the data protection is taken, may require an active investigation of the supervisory bodies and cooperation with them.

The administrative burden lies at the controllers and processors. They have to be able to demonstrate where they accept and fulfil the relevant decisions. All this has to be recorded so that the records could help to identification of a lead supervisory authority.

- Also in the case of identification of lead supervisory authority, it is possible for the other supervisory bodies to step into the data processing and lead the investigations.

SPCR comment: It is obvious from the above said, that "One-Stop-Shop" is a pure fiction. In the modern age of diversified activities, projects and more linear than hierarchic leadership, the case of "One-Stop-Shop" will apply to a minimum companies as in a minimum of cases, only one entity takes decision about all the data processing activities. The only identification of a lead supervisory authority or clearing which authorities will be needed to cooperate with, will be very much administratively complicated – another raising of bureaucracy, more expensive and less effective development of the new products and services. The companies are therefore forced to create centres with concentration of decision-making processes in EU.