CONFEDERATION OF INDUSTRY
OF THE CZECH REPUBLIC

PRAGUE, 28 NOVEMBER 2017

Position to the material of Article 29 Working Party: Guidelines on Personal data breach notification under Regulation 2016/679

INTRODUCTION

The duty of data controller to notify data breaches to the competent national supervisory authority (further referred as "DPA") is one of the remarkable news in the field of data protection processing and administration introduced into the Czech legal environment by the General Data Protection Regulation (further referred as "GDPR" only). It implies many questions of Czech data controllers on how the duty should be properly applied, in what form, how to ensure that the data controller is informed about the data breach in a real time and what could be the risks of referring about the data breach to the DPA as well as to the data subjects in terms of communicating, together with notifying the data breach, also the related sensitive information of data controllers' organisation.

These procedures present remarkable new administrative burden for the Czech data controllers as well as certain legal uncertainty; however, the Commission, when presenting GDPR Proposal, has not paid enough attention to this new burden and has not evaluated the potential impacts of GDPR in this field. This context of the new duty, therefore, causes certain constraint at the side of Czech data controllers: especially those who are not subject to notification duties according to the other EU regulation[1] are sometimes getting informed about this new duty with a remarkable delay and in the very last minute before entering GDPR into force. In this situation, they seek for clear and understandable guidance precising their obligations and offering possible simple recipes how to get compatible with their duties arising from GDPR.

We are, therefore, expecting from the present WP 29 Guidelines to answer these questions and, especially, to give the data controllers a comprehensive guide, how to at one side fulfil properly their duties connected with data breaches notifications according to GDPR and, at the opposite, not to open their back to possible concurrence and not to make their sensitive information, know-how and business secret public.

Following the publication of the present Guidelines 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 3th October 2017, Confederation of Industry of the Czech Republic (further referred as "SP CR") would like to make the following comments to the published document:

[1] e.g. the NIS Directive.

PHONE (+420) 225 279 111 | E-MAIL SPCR@SPCR.CZ
WEB WWW.SPCR.CZ | ADDRESS FREYOVA 948/11, 190 00 PRAGUE 9, CZECH REPUBLIC

INTRODUCTORY REMARKS OF SP CR

- *Within its interpretational Guidelines, WP29 explains that the new notification requirement has a number of benefits[2] because, when notifying the supervisory authority, the controller can obtain advice on whether (and in what way) the affected data subjects need to be informed. By informing the data subjects, the controller can, according to WP29 opinion, by providing information on the risks resulting from the breach, help the data subjects to protect them against potential harm. However, WP29 does not take into account the situation of data controller – the notification duty may disclose its weaknesses and vulnerabilities even before the data controller can manage to solve the consequences of the breach and to take steps to reinforce his measures to ensure security to the controlled personal data.* ***It would have been better to explain that, firstly, the notification to DPA should be done and later, only after ensuring that the publication of the breach is secure enough and cannot cause any further harm, the notification to data subjects should be realized.***

- *WP29 in the present Guidelines admits that* ***information required for the notification can be provided in phases, but in any event controllers should act on any breach in a timely manner****.[3] This is a very important point for data controllers who are not sure whether to focus better on a quick, but still incomplete, notification or to wait with the notification until the basic parameters of the breach are known. We therefore reckon that more "the quick notification counts" and will be counted as more earnest approach of the data controller than completion of information about the breach. However,* ***we would like to prevent WP29 from assessing that a possible investigations about the full content and reach of data breach could or should be only a question of a short time*** *immediately following after the first moment after the data controller gets informed about a data breach: the opposite may be true in many cases and, therefore, it is unfair to presume automatically that the investigation should be realized and closed in a very short time after the controller getting informed about the breach, as it is visible from Section II. A 2. of the present Guidelines.[4]*

- *The types of personal data breaches are being divided into 3 types, according to the three information security principles: confidentiality, availability and integrity breach[5] and all its possible combinations including a "triple" breach containing all the three negative cases at once.* ***However, it is not correct to imply that a sole temporarily unavailability of data can be considered as a data breach[6]****. This goes beyond the scope of the text of GDPR and, therefore, this kind of interpretation should be abandoned. In this regard, it is not relevant that WP29 reasonably answers some of the related questions admitting that, in this situation, it depends on the circumstances if the incident may or may not require notification to DPA and communication to the involved data subjects, according to the fact if the lack of data availability is likely or not likely to result in a risk to the rights and freedoms of natural persons.[7] This situation simply does not present a data breach and, therefore, it should be excluded from the present Guidelines.*

---

[2] Page 4 of the present Guidelines.

[3] Page 5 of the present Guidelines.

[4] See bottom of page 9 and page 10 of the present Guidelines.

[5] See page 6 of the present Guidelines.

[6] See page 7 of the present Guidelines.

[7] See page 7 of the present Guidelines.

- *The Guidelines describe that the negative effects on individuals caused by a breach can vary from physical through material up to non-material damage.*

- *It is important to acknowledge that the failure to notify the data breach may sometimes reveal even more serious infringement of the controller's obligations, mainly the obligations to undertake appropriate security measures to protect the controlled data. In this case, the Guidelines admit that the DPA can issue sanctions for both these infringements made by the data controller.*[8] ***It is in place, therefore, to prevent the data controllers that failure to fulfil the notification duty may present an evidence of even more serious breach of their duties imposed by GDPR.***

- *WP29 concludes, regarding the consideration of the moment when the controller becomes "aware" that, i.e. when losing a CD with sensitive data, the controller with no doubt becomes aware of the data breach in the moment when it realizes the CD has been lost. However, this description is a little bit schematic:* ***the data controller is very often a legal person, being in a position of employer towards the persons who may potentially, in their position of employees, physically cause the data breach. What should be the procedure of notification between the employees as the persons causing the data breach and the data controller as their employer? Who could ensure that the data controller gets in a real time information about the certain data breach? WP29 does not answer these questions*** *– however, in a real life, we reckon that this situation will be very often.*

- *The Guidelines explain in a comprehensive and understandable way how the relationship between data controllers and processors should be regulated and what principles are to be fulfilled within data breaches notifications.*[9] ***Not surprisingly, the Guidelines alert that the overall responsibility for data breach notification and its communication to the respective data subjects lies at the data controller*** *and, therefore, the controllers are required to specify how the procedure of a sub-notification of a breach from the data processor to the controller should be made, within their contracts with their processors.*

- *In the part dedicated to the communication of the breach to the data subject, WP29 emphasizes the well-known fact that the threshold for communicating a breach is higher than for notifying supervisory authorities – there should exist a high risk to the rights and freedoms of the individuals. WP29 also in a comprehensive way explains that a description of the nature of the breach, name and contact details of DPO or another responsible person of the data protection controller, description of possible consequences and measures taken or proposed to be taken by the controller. Until now, the description of the duty by WP29 is clear and transparent, not widening the scope of GDPR. However, when explaining the possible means of communication to the data subjects, WP 29 deduces that examples of transparent communication include direct messaging (email, SMS, another direct message) or prominent website banners, postal communication and prominent advertisements in printed media.* ***We reckon that it is pity that it omits the easiest possible way of communication – website or social networks accounts of the data controller****. It also enhances the administrative burden of a controller by describing that* ***communication in the native language of the recipient will***

[8] See page 8 of the present Guidelines.

[9] See page 11 of the present Guidelines.

help to ensure their understanding of the nature of the breach.[10] ***These two points might lead to excessive new burden to the data controller and are widening the scope of GDPR.***

- *It is in place to* ***appreciate that WP29 takes into account the relevant interpretational tools drafted by other relevant actors; i.e****. it recommends to the attention of data controllers the relevant recommendations for a methodology of assessing the severity of a breach by the* ***European Union Agency for Network and Information Security (ENISA).***

- *In the present Guidelines, WP29 prevents that there are also some other notification duties under other relevant legislation, especially the duty of trust service providers to notify their supervisory authority of a breach under eIDAS Regulation and operators of essential services and digital services providers are required to notify security incidents under NIS Directive.* ***It should have been a good administrator's practice from WP29 to offer to the supervisory authorities, as a good example practice, to offer a unified or at least compatible form of such a breach notification to the data controllers (who could be in the same time in a position of a trust service provider or an essential service operator). However, WP29 does not show such an initiative.***

Following this general evaluation, SP CR further formulates its recommendations which should, according to our opinion, lead to the revision of the present Guidelines so that it will ensure better applicability of GDPR, mainly in the practice within enterprises. In the same time, we use this opportunity to comment the proposed text of the Guidelines with the aim to attract the attention to some unclear points and, therefore, to eliminate the possible negative impacts of the Guidelines.

SPECIFIC COMMENTS:

According to our opinion, WP29 goes outside the scope of GDPR in the following points:

1. ***Explanation of the means of communication of the data breach to the data subjects/natural persons involved:*** *WP 29 deduces that examples of transparent communication include direct messaging (email, SMS, another direct message) or prominent website banners, postal communication and prominent advertisements in printed media. Therefore, it* ***implicitly excludes the easiest possible way of communication – website or social networks accounts of the data controller****. It also enhances the administrative burden of a controller by describing that* ***communication in the native language of the recipient will help to ensure their understanding of the nature of the breach****. This both (description of the means of communication as well as of the language of the communication) goes beyond the scope of GDPR and this kind of interpretation should be abandoned.*

2. ***Including also the <u>temporary</u> unavailability of data into the list of data breaches****: this goes beyond Art. 4 par. 2 GDPR, where no note about temporary availability of data is being made, and so it is in all the other text of GDPR. Temporary unavailability of data presents, with no doubt, a security incident, but could not be considered as data breach causing all the consequent duties of a data controller (notification, communication and documentation). Exclusion of all the notes about "temporary unavailability", see among our recommendations below.*

[10] See page 18 of the present Guidelines.

3. ***Presuming that a data controller is immediately informed about a data breach occurred within the data processing by a processor supplying its services to the data controller:*** *WP29 in the present Guidelines presents that "The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as "aware" once the processor has become aware." This presumption is roughly incorrect and arises from the unawareness of WP29 about the practical procedures within data processing and relationships between data controllers and their processors. In practice, this is hardly ever true and, in most cases, the situation is exactly opposite: the data controller hardly ever gets immediately informed about a data breach occurred within the data processing by a processor and, therefore, it is incorrect to presume that the moment when the processor becomes aware of a data breach is the same when the controller becomes aware as well. From this incorrect presumptions, other incorrect conclusions of WP29 arise and, therefore, we propose to reassess this approach and the consequent recommendations of WP29.*

RECOMMENDATIONS:

Following the aforementioned points, SP CR recommends to:

1. ***Modify the description of an availability breach in Section I.B.2 on page 6*** *to: "Availability breach – where there is an unauthorised or accidental loss or destruction of personal data," which is consistent the Article 4(12).*

2. ***Delete "temporarily" from the second paragraph in the example box at the top of page 7****, have the final text as follows: "A loss of availability may also occur where there has been significant disruption to the normal service of an organisation, for example, experiencing a power failure or denial of service attack, if it renders personal data permanently unavailable.*

3. ***In the second paragraph following the first example box on page 7, modify the next-to-last sentence*** *as such: "If the lack of availability of personal data is permanent and is likely to result in a risk to the rights and freedoms of natural persons, then the controller will need to notify."*

4. ***Either delete the second example box on page 7, or modify the examples to reflect that they both involve the temporary unavailability of data****, which would constitute a security incident but not an Article 4(12) data breach.*

5. ***Consider updating the first example in the box on page 9 and example i. on page 27, by replacing the lost CD with a lost USB key*** *or adding the latter to the example, to align it with current practices.*

6. ***Delete "short" from the phrase "short period of investigation" in the paragraph at the bottom of page 9 and in the box on page 10, and "brief" from "brief period of investigation" at the top of page 11****. The importance of notifying without undue delay might be emphasized in other ways without unrealistically asserting that all initial investigations of security incidents will be "short."*

7. ***Delete the sentence that makes up the second paragraph at the top of page 10****: "In most cases the preliminary actions should be completed soon after the initial alert – it should take longer than this only in exceptional cases." As our discussion of the problems with the examples above*

indicates, even in a seemingly obvious case like a lost CD some time for investigation is necessary to discover the facts necessary to make a determination of "notifiability."

8. ***Delete the second sentence in paragraph 2 of Section II.A.3 on page 11****: "The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as "aware" once the processor has become aware." Replace the deleted sentence with a statement of a controller's discretion to contractually prescribe the practices its processors must follow in notifying the controller of a potential personal data breach detected by the processor, with notification of the controller required to occur no later than when a processor has become "aware" of the breach (i.e., has conducted an initial investigation and found that the breach is likely to pose a risk to individual rights and freedoms).*

9. ***In paragraph 3 of Section II.A.3 on page 11****: Add a statement explaining that a phased notification by a processor to a controller would enable the controller to participate in or oversee the processor's initial investigation.*

10. ***In paragraph 5 of Section II.A. on page 11****: Add to the beginning of the first sentence the phrase: "In the case of a breach originating with the processor…"*

11. ***In paragraph 5 of Section II.A. on page 11:*** *Add a recommendation that joint controllers should contractually provide for notification responsibilities in the case of a personal data breach affecting a jointly managed system.*

12. ***Accomplish the Section VI. Notification obligation under other legal instruments:*** *To include a text explaining that it would present a good practice example from the part of data supervisory authorities as well as from the part of other supervisory bodies to develop a unified or at least compatible form of a breach notification according to GDPR together with eIDAS Regulation, NIS Directive (and possible other legal instruments implying the notification duty on certain subjects).*

13. ***Delete the point "the number of affected individuals" (Section IV.B, page 22)*** *and the following discussion of it as one of the criteria for assessing the risk that a personal data breach poses to the rights and freedoms of data subjects [as the mere number does not determine the individual risk].*

14. ***Modify the Flow Chart in Annex A on page 26:*** *In the box in the left column on notifying the supervisory authority, delete the second sentence (on notifying authorities in all Member States) and change the first so that it reads: "Notify competent supervisory authority(ies)."*

15. ***Accomplish the Flow Chart in Annex A on page 26:*** *Clarify that a controller that does not have an establishment in the EU may notify the supervisory authority where its representative is located, in addition to the authority where the breach occurred.*

16. ***Modify breach Example ii on page 27*** *to eliminate the term "potential" and add a consideration of the factor of likelihood.*
    The advice on notifying the supervisory authority could be as follows: "Report to competent supervisory authority if adverse consequences to individuals are likely."
    The advice on notifying the data subject could be: "Communicate to individuals if there is a likelihood of severe adverse consequences." The notes section could also be changed to acknowledge consideration of the likelihood factor.

17. ***Modify Example Breach iv on page 28****. In the answer to question of notifying the supervisory authority, change "potential" to "likely." In the answer to the question of notifying the data subjects, change the language to include assessing the likelihood of risk, to read: "Yes, report to individuals, depending on the likelihood of the lack of availability of the personal data having serious consequences for individuals."*

18. ***Modify breach Example vi on page 29*** *to reference both the likelihood and severity of consequences.*

    The advice on notifying the supervisory authority could be texted as follows: "Report to lead supervisory authority, because the cyber-attack indicates intention to harm, thus creating likelihood, and adverse consequences cannot be adequately mitigated."

    The advice on notifying to data subjects could be: "Communicate to data subjects because there is both likelihood and, depending on the specific data involved, severity of consequences. In any case, inform data subjects about changing their account credentials." The notes could advise on mitigation actions the controller should take.