# Comments regarding Guidelines 01/2021 on Examples regarding Data Breach Notification, Version 1.0, adopted on 14 January 2021

******

**Introduction**

Floreani Studio Legale Associato welcomes the opportunity to provide a response to the European Data Protection Board's consultation on the drafts Guidelines 01/2021 on Examples regarding Data Breach Notification and invites the EDPB to evaluate the following proposals as well as to clarify the problems highlighted below.

**1 INTRODUCTION**

**Para. 7: "*Accordingly, the GDPR requires the controller to:***

- ***document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken;***
- ***notify the personal data breach to the supervisory authority, unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons;***
- ***communicate the personal data breach to the data subject when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons".***

**Comment:** We suggest the EDPB to mention in the Guidelines the case which the "*processor could make a notification on behalf of the controller, if the controller has given the processor the proper authorisation and this is part of the contractual arrangements between controller and processor"* (*Guidelines on Personal data breach notification under Regulation 2016/679,WP250 rev.01, 6 February 2018, p. 14*).

**Para. 8: "*Data breaches are problems in and of themselves, but they are also symptoms of a vulnerable, possibly outdated data security regime, thus indicate system weaknesses to be addressed".***

**Comment:** It should be noted that personal data breaches are not necessarily a direct consequence of an outdated data security regime, being a problem inherent in the use of computer systems and / or devices containing personal data. We propose the EDPB to evaluate the opportunity to reformulate the provision in question.

**Para. 9: "*The breach should be notified when the controller is of the opinion that it is likely to result in a risk to the rights and freedoms of the data subject. Controllers should make this assessment at the time they become aware of the breach. The controller should not wait for a detailed forensic examination and (early) mitigation steps before assessing whether or not the data breach is likely to result in a risk and thus should be notified".***

**Comment:** We propose the EDPB to evaluate the opportunity to indicate the possibility for data controllers to also make use of the self-assessment procedures made available by the SAs.

**Para. 13: "*The principle of accountability and the concept of data protection by design could incorporate analysis that feeds into a data controller's own "Handbook on Handling Personal Data Breach" that aims to establish facts for each facet of the processing at each major stage of the operation. Such a handbook prepared in advance would provide a much quicker source of information to allow data controllers to mitigate the risks and meet the obligations without undue delay. This would ensure that if a personal data breach was to occur, people in the organisation would know what to do, and the incident would more than likely be handled quicker than if there were no mitigations or plan in place".***

**Comment:** With reference to the highlighted paragraph, we propose the EDPB to specify the drafting criteria of the data controller's own "Handbook on Handling Personal Data Breach"and that the contents may include the best practices indicated in the Guidelines, adapting the risk identification and mitigation processes to the reality of the organization.

**2 RANSOMWARE**

**2.4 CASE No. 04: Ransomware without backup and with exfiltration**

**2.4.2 CASE No. 04 – Mitigation and obligations**

**Para. 47: "*(…) The latter could be undertaken on a person-by-person basis, but for individuals where contact data is not available the controller should do so publicly, e.g. by way of a notification on its website. In the latter case a precise and clear communication is required, in plain sight on the homepage of the controller, with exact references of the relevant GDPR provisions. The organisation may also need to update and remediate its organizational and technical personal data security handling and risk mitigation measures and procedures".***

**Comment:** We ask the EDPB in the case in which the data controller does not have a website and if the contact details of the data subjects are not available - to identify alternative ways

to communicate the breach and indicate the provisions of the Board to page 22 of the Guidelines on Personal data breach notification under Regulation 2016/679,WP250 rev.01, 6 February 2018: "*Whenever it is not possible for the controller to communicate a breach to an individual because there is insufficient data stored to contact the individual, in that particular circumstance the controller should inform the individual as soon as it is reasonably feasible to do so (e.g. when an individual exercises their Article 15 right to access personal data and provides the controller with necessary additional information to contact them").*

**2.5 Organizational and technical measures for preventing / mitigating the impacts of ransomware attack**

**Para. 49: "*Advisable measures: (The list of the following measures is by no means exclusive or comprehensive. Rather, the goal is to provide prevention ideas and possible solutions. Every processing activity is different, hence the controller should make the decision on which measures fit the given situation the most.)."***

**Comment:** We suggest the EDPB to mention in the Guidelines some further practical solutions and advice on the terms of release from attack ransomware (for example, also contact specialized technicians able to unlock the device; report the ransomware attack to the Postal Police).

**4 INTERNAL HUMAN RISK SOURCE**

**4.1 CASE No. 08: Exfiltration of business data by a former employee**

**4.1.1 CASE No. 08 - Prior measures and risk assessment**

**Para. 73: *"As usual, during risk assessment the type of the breach and the nature, sensitivity, and volume of personal data affected are to be taken into consideration. These kinds of breaches are typically breaches of confidentiality, since the database is usually left intact, its content "merely" copied for further use. The quantity of data affected is usually also low or medium. In this particular case no special categories of personal data were affected, the employee only needed the contact information of clients to enable him to get in touch with them after leaving the company. Therefore, the data concerned is not sensitive".***

**Comment**: We propose the EDPB to evaluate the opportunity to reformulate the example shown. In this case, it cannot be excluded that the database copied by the ex-employee also contains special categories of personal data and sensitive information of the company's clientele.

**4.1.2 CASE No. 08 – Mitigation and obligations**

**Para. 76:** ***"There is no "one-size fits-all" solution to these kinds of cases, but a systematic approach may help to prevent them. For example, the company may consider – when possible - withdrawing certain forms of access from employees who have signalled their intention to quit or implementing access logs so that unwanted access can be logged and flagged. The contract signed with employees should include clauses that prohibit such actions".***

**Comment**: It is suggested to the EDPB to specify the importance of regulating the legitimate use of data by employees by issuing specific instructions on the processing and clauses that provide for the obligation to return data at the end/interruption of the employment relationship and the prohibition of retention, copying and use of databases.

**4.2 CASE No. 09: Accidental transmission of data to a trusted third party**

***"An insurance agent noticed that – made possible by the faulty settings of an Excel file received by e-mail – he was able to access information related to two dozen customers not belonging to his scope. He is bound by professional secrecy and was the sole recipient of the e-mail. The arrangement between the data controller and the insurance agent obliges the agent to signal a personal data breach without undue delay to the data controller. Therefore, the agent instantly signalled the mistake to the controller, who corrected the file and sent it out again, asking the agent to delete the former message. According to the above-mentioned arrangement the agent has to confirm the deletion in a written statement, which he did. The information gained includes no special categories of personal data, only contact data and data about the insurance itself (insurance type, amount). After analysing the personal data affected by the breach the data controller did not identify any special characteristics on the side of the individuals or the data controller that may affect the level of impact of the breach".***

**Comment**: With respect to the provision in question, it may be appropriate for the EDPB to clarify in the example shown, the details of the data controller.

**4.2.2 CASE No. 09 – Mitigation and obligations**

**Para. 82: "***Besides documenting the breach in accordance with Article 33 (5), there is no need for any other action".*

**Comment**: With reference to the paragraph in question, we propose the EDPB to specify in the Guidelines that the obligations to document the breach in accordance with article 33 (5) are the responsibility of the data controller.

**5 LOST OR STOLEN DEVICES AND PAPER DOCUMENTS**

**5.3 CASE No. 12: Stolen paper files with sensitive data**

**5.3.2 CASE No. 12 – Mitigation and obligations**

**Para. 102: "*During the assessment of the safeguarding measures the type of the supporting asset should be considered as well. Since the patient log book was a physical document, its safeguarding should have been organized differently than that of an electronic device. The pseudonymisation of the patients' names, the storage of the book in a safeguarded premises and in a locked drawer or a room, and proper access control with authentication when accessing it could have prevented the data breach".***

**Comment:** We ask the EDPB to specify the organizational measures to protect personal data contained in physical documents with the use of further practical examples.

**7 OTHER CASES – SOCIAL ENGINEERING**

**7.1 CASE No. 17: Identity theft**

**7.1.1 CASE No. 17 - Risk assessment, mitigation and obligations**

**Para. 128: "*Instead, the organisation should use a form of authentication which would result in a high degree of confidence that the authenticated user is the intended person, and not anyone else. The introduction of an out-of-band multi-factor authentication method would solve the problem, e.g. to verify the change demand, by sending a confirmation request to the former contact; or adding extra questions and requiring information only visible on the previous bills. It is the controller's responsibility to decide which measures to introduce, as it knows the details and requirements of its internal operation the best".***

**7.2 CASE No. 18: Email exfiltration**

**7.2.1 CASE No. 18 - Risk assessment, mitigation and obligations**

**Para. 131: "*The fact that a breach could happen and go undetected for so long and the fact that, in a longer time, social engineering could have been used for altering more data, highlighted significant problems in the controller's IT security system. These should be addressed without delay, like emphasizing automation reviews and change controls, incident detection and response measures. Controllers handling sensitive data, financial***

***information, etc. have a larger responsibility in terms of providing adequate data security".***

**Comment**: In this regard, we ask the EDPB to evaluate the opportunity to specify in the Guidelines a non-exhaustive list of organizational and technical measures for preventing/ mitigating the impacts of identity theft and business email compromise (BEC).

**Comment:** With reference to the examples reported in paragraph 7, it might be appropriate for the EDPB to formulate some further cases (for example, SIM-swap; vishing; pharming).

We would be grateful for your consideration of our comments and proposals and remain available for any clarification and further information.

Sincerely.

01 March 2021