PUBLIC CONSULTATION - "Guidelines 1/2021 on Examples regarding Data Breach Notification"

COMMENTS BY	
SERGIO	GUIDA
Independent Researcher, Sr. Data Governance & Privacy Mgr.	
E-mail: risk_management@fisicagestionale.com	

PAGE	TEXT	COMMENTS
5	(1 INTRODUCTION) 6. A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymization, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy.	**Here it would be useful to include references to the ENISA's Guidelines on Data Pseudonymization in a footnote.**

6	(1 INTRODUCTION) 8. .. In other cases the notification does not need to be postponed until the risk and impact surrounding the breach has been fully assessed, since the full risk assessment can happen in parallel to notification, and the information thus gained may be provided to the SA in phases without undue further delay.	**It would be advisable to provide, if not a rule, at least some examples relevant to circumscribe the notion of "undue further delay" in both causal and temporal terms.**
8	(2 RANSOMWARE) 19. When assessing the risks, the controller should investigate the breach and identify the type of the malicious code to understand the possible consequences of the attack. Among those risks to be considered is the risk that data was exfiltrated without leaving a trace in the logs of the systems.	**Apparently it is difficult to see something that leaves no trace, so one must prevent data exfiltration with security solutions. It would be useful remember, in a footnote, e.g., firewalls to block unauthorized access to resources and systems storing sensitive information, or a security information and event management system (SIEM) to secure data in use, and at rest, secure endpoints, and identify suspicious data transfers.**
9	(2 RANSOMWARE) 24. The timeliness of an effective data restoration from the readily available backup is a key variable when analysing the breach. Specifying an appropriate timeframe to restore the compromised data depends on the unique circumstances of the breach at hand. The GDPR states that a personal data breach shall be notified without undue delay and, where feasible, not later than after 72 hours. Therefore, it could be determined that exceeding the 72-hour time limit is unadvisable in any case, but when dealing with high risk level cases, even complying with this deadline can be viewed as unsatisfactory.	**In some cases such as those exemplified just further on in the document, it appears clearly how the notification must be made immediately, as soon as the data controller has come aware of the data breach.**

10	(2 RANSOMWARE) 33. The restoration of the data should not prove to be overly problematic 12 if the data is still available on paper, but given the lack of an electronic backup database, a notification to the SA is considered necessary, as the restoration of the data took some time and could cause some delays in the orders' delivery to customers and a considerable amount of meta-data (e.g. logs, time stamps) might not be retrievable.	**As both in the paragraph text and in the footnote the importance of metadata is reiterated, then it would be useful to remember also why consistency with metadata is so relevant for verification.**
13	(2.5 Organizational and technical measures for preventing / mitigating the impacts of ransomware attacks) 48. The fact that a ransomware attack could have taken place is usually a sign of one or more vulnerabilities in the controller's system. This also applies in ransomware cases in which the personal data has been encrypted, but has not been exfiltrated. Regardless of the outcome and the consequences of the attack, the importance of an all-encompassing evaluation of the data security system - with particular emphasis on IT security - cannot be stressed enough. The identified weaknesses and security holes are to be documented and addressed without delay.	**So why not introduce a periodic obligation of evaluation, e.g. yearly, paid by the data controller?**
14	(49. Advisable measures:) Forwarding or replication all logs to a central log server (possibly including the signing or cryptographic time-stamping of log entries).	**And why not introduce a periodic obligation e.g. on a weekly basis?**

14	(49. Advisable measures:) When assessing countermeasures – risk analysis should be reviewed.	**It might be useful to test and update, if necessary, the connections to the DPIA as well.**
20	(4 INTERNAL HUMAN RISK) 75. The mitigation of the adverse effects of the breach in the above case is difficult. It might need to involve immediate legal action to prevent the former employee from abusing and disseminating the data any further. As a next step, the avoidance of similar future situations should be the goal. The controller might try to order the ex-employee to stop using the data, but the success of this action is dubious at best.	**In addition to legal measures such as, for example, signing non-competition agreements, for the profiles of employees for which a formal notice of resignation or dismissal has been provided, I would also and above all adopt technical measures such as the impossibility of copying or downloading data on their own devices or memories.**