



ARTICLE 29

Data Protection Working Party

Data Breach Notification under Regulation 2016/679

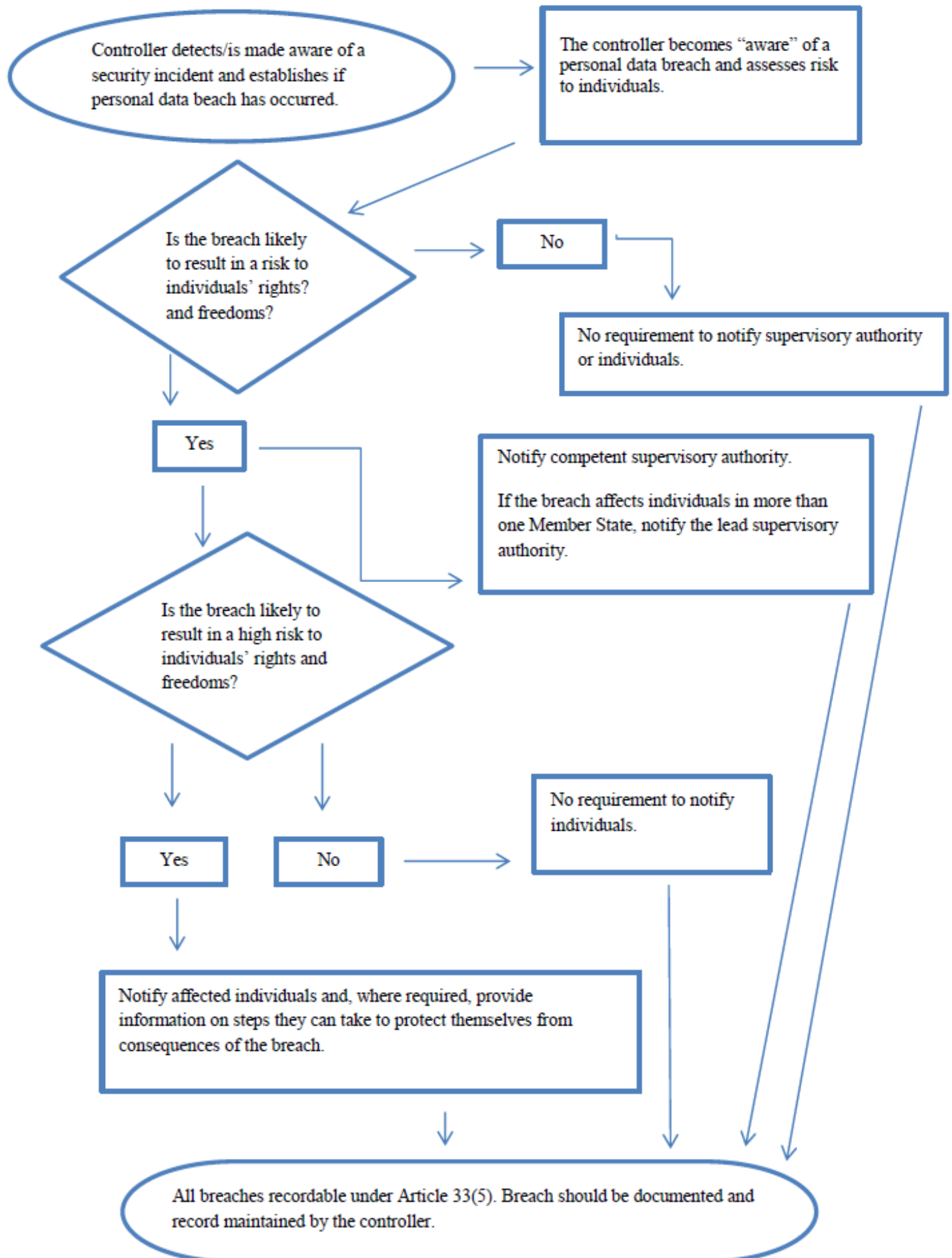
Extract From Article 29 Working Party 03rd October 2017

Access Reference 18/EN WP25rec.01

Document Link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

VII. Annex

A. Flowchart showing notification requirements



B. Examples of personal data breaches and who to notify

The following non-exhaustive examples will assist controllers in determining whether they need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	Notify the supervisory authority?	Notify the data subject?	Notes/recommendations
i. A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required.
ii. A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated. The controller has customers in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
iii. A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
iv. A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or

<p>functionality was to encrypt the data, and that there was no other malware present in the system.</p>		<p>consequences.</p>	<p>confidentiality. However, if the supervisory authority became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.</p>
<p>v. An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else.</p> <p>The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.</p>	<p>Yes.</p>	<p>Only the individuals affected are notified if there is high risk and it is clear that others were not affected.</p>	<p>If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.</p>
<p>vi. A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.</p>	<p>Yes, report to lead supervisory authority if involves cross-border processing.</p>	<p>Yes, as could lead to high risk.</p>	<p>The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk.</p> <p>The controller should also consider any other notification obligations, e.g. under the NIS Directive as a digital service provider.</p>
<p>vii. A website hosting company acting as a data processor identifies an error in the code which</p>	<p>As the processor, the website hosting company must notify its affected clients (the controllers) without</p>	<p>If there is likely no high risk to the individuals they do not need to be</p>	<p>The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS</p>