Example	Notify the ICO?	Notify the Data Subject?	Recommendations from European Data Protection Board Oct 2017
Controller stored a backup of an archive of personal data encrypted on a CD. The CD 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, and the unique key is not compromised, this may not be a reportable breach unless later compromised
Personal data of individuals are exfiltrated from a secure website manage by the controller during a cyber-attack. The controller has customers in the UK only.	Yes, report to ICO if there are potential consequences	Yes, report to individuals depending on the nature and severity of the personal data affected	If the risk is not high, it is recommended the controller to notify the data subject depending on the circumstances. Eg. If a newsletter related to a political event resulting in a political point of view being disclosed
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	It is a recordable incident and appropriate records should be maintained by the controller.
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 functionality was to encrypt the data and that there was no other malware present in the system.	Yes, report to ICO if there a potential 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 consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the ICO or individuals as there would have been no permanent loss of availability or confidentiality. However, the ICO may consider an investigation to assess compliance with the broader security requirements of Article 32.
An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (within 24 hrs) and establishes with a reasonable confidence that a personal data breach has occurred and if it is a systemic flaw so that other individuals are or might be affected.	Yes	Only if the individuals affected are notified if there is a high risk and it is clear that others were not affected.	If after further investigation, it is identified that more individuals are affected, an update to the ICO is required and the controller takes the additional step of notifying other individuals if there is high risk to them.
A multi-national online marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker	Yes, report to ICO or the lead supervisory authority if it involves cross-border processing.	Yes as could lead to high risk	The controller should take action eg by forcing password resets of the affected accounts, as well as other steps to mitigate the risk.
A website hosting company (data processor) identifies an error in the code which controls user authorisation. The effect of the flaw means	The processor must notify its clients (controller) without undue delay. Assuming that the	If there is likely no high risk to the individuals they do not need to be notified.	The website hosting company (processor) must consider any other notification obligations (eg under the NIS Directive).

that any user can access the account details of any other user.	website hosting company has conducted its own investigation, the controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having 'become aware' once they have been notified by the processor. The controller then must notify the ICO.		If there is no evidence of this vulnerability being exploited with this controller a notifiable breach may not have occurred but is likely to be recordable or be a matter of non-compliance under Article 32.
Medical records in a hospital are unavailable for the period of 30hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to affected individuals.	
Personal data of 5000 students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes report to ICO	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
A direct marketing email is sent to recipients in "to" or "cc" field thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the ICO may be obligatory if a large number of individuals are affected, if sensitive data are revealed (eg mailing list of psychotherapist) or if other factors present high risks (eg the mail contains the initial passwords)	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.