Overview Data Breach Notifications

	Current FADP	Draft FADP	GDPR
Notification to Data Protection Authority			
Which incidents must be reported?	No express notification obligation.	Data security breach[1] that is probable to result in a high risk to privacy or fundamental rights of data subject.	Every personal data breach[2] unless it is unlikely to result in a risk to the rights and freedoms of the data subject.
To whom?		Federal Data Protection and Information Commissioner (FDPIC).	Supervisory authority of the main establishment or of the only affected single establishment.
Time limit?		As soon as possible.	Without undue delay, in general within 72 hours.
Notification to Data Subject			
Which incidents must be reported?	No express notification obligation, but might result from general data processing principles.	Data security breach if notification is necessary for the protection of the data subject or if the FDPIC so requests.	Personal data breach with high risk to the rights and freedoms of natural persons.
To whom?		Every single affected individual or in an equivalent manner by public announcement.	Every single affected individual, if disproportionate than communication to public.
Time limit?		No specific requirement.	Without undue delay.
Documentation Duty			
	No express documentation obligation.	No express documentation obligation.	Every data breach must be documented.
Sanctions for Noncompliance with Notification or Documentation Duties?			
	None.	None.	Fines up to EUR 10 million or 2 % of worldwide annual turnover.

Depending on the field of activity of the company, duties to notify sector-specific authorities may exist.

[1] "Data security breach" means a security breach, irrespective of whether is intentional or unlawful, which leads to a loss, deletion, destruction or modification of personal data or to personal data being disclosed or made accessible to unauthorised persons (article 4 (g) draft FADP).

[2] "Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (article 4 (12) GDPR).