

International Data Privacy Principles

- *Developed by Wolfgang Zankl, Vienna*
- *Based on a contractual balance approach with consideration of American, Asian, European and International Data Protection Standards*
- *Discussed with Harvard University (Boston) and Computer Ethics Society (Hong Kong)*

Companies in compliance with International Data Privacy Standards commit to

- (1) complying with national data protection or privacy law, national contract law and other legal requirements or regulations referring to data privacy
- (2) complying with current security standards to protect stored personal data from illegitimate or unauthorised access or from accidental access, processing, erasure, loss or use
- (3) implementing an easily perceptible, accessible and comprehensible privacy policy with information on who is in charge of data privacy and how this person can be individually contacted, why and which personal data is collected, how this data is used, who will receive this data, how long this data is stored, whether and which data will be deleted or rectified upon request
- (4) instructing employees to comply with such privacy policies and to avoid activities which enable or facilitate illegitimate or unauthorized access in terms of paragraph 2
- (5) not using or divulging any customer data (except for statistical analysis and when the customer's identity remains anonymous) unless the company is obliged to do so by law or the customer agrees to such use or circulation
- (6) not collecting customer data if such collection is not necessary or excessive
- (7) using or divulging customer data in a fair way, for a purpose related to activities of the company
- (8) not outsourcing customer data to third parties unless they also comply with International Data Privacy Standards
- (9) announcing data breaches regarding sensitive data (referring to, e.g., sexual, financial, medical, political, ethnic or religious issues)
- (10) not keeping personal data for longer than necessary
- (11) not transferring personal data to countries with inadequate or unknown data protection standards

(12) in case of a contract between the company and the customer committing the customer to pay for services or goods:

- informing the customer individually and as soon as reasonably possible in case of data breaches with regard to personal data
- informing the customer upon request about which specific data of this customer is stored and deleting such data upon request unless applicable laws or regulations require the company to continue storing such data
- not using or divulging content-related personal data
- not using or divulging any other personal data without the customer's explicit, separate and individual consent
- not storing, using or divulging any customer data whatsoever when all or part of the customer's payment is charged by the company for not storing, using or divulging customer data unless applicable laws or regulations require the company to continue storing such data

(13) in the absence of a contract between the company and the customer committing the customer to pay for services or goods:

- informing the customer as soon as reasonably possible in case of data breaches with regard to sensitive data
- informing the customer upon request what type of sensitive data of this customer is stored and deleting such data upon request when such data is outdated unless applicable laws or regulations require the company to continue storing such data
- not using or divulging sensitive data without the customer's explicit, separate and individual consent

