

Exercices “Laws, Regulations, and Privacy Seals”

Exercice 1:

Pick a (Web) company and study their privacy policies. What are their strong and weak points? You may use the template given in <http://www.privacy.gov.au/publications/seals.html#412>. What about Facebook or Google?

Exercice 2:

What is the difference between the two privacy seals of SQS (Schweizerische Vereinigung für Qualitäts- und Management-Systeme) <http://www.sqs.ch> and TÜV SÜD Management Service GmbH <http://www.safer-shopping.de> ?

Solution:

	Good Priv@cy	S@fer Shopping
Founded	?	2001
Assurance organization	SQS, founded in 1983, is a non-profit organisation. It has 135 permanent employees in Switzerland, France and Italy and 252 independent employees worldwide.	TÜV SÜD Management Service GmbH
Assessment organization	SQS, SQS-lead-auditor	TÜV SÜD Management Service GmbH
Service	Certification of a data protection management system with respect to the relevant national legal requirements, internal and contractual agreements as well as the corresponding information security.	Certification of technical and operational procedures. Own requirements catalog.
Checking procedure	?	self assessment, scanning of Web pages, local audit
Oversight procedure	?	?
Validity	3 years	unlimited
Ongoing monitoring	yearly	yearly
Resolution procedure	?	yes
# Participants	28	60
Licensees	Migros, Photocolor Kreuzlingen AG, Schaden Service Schweiz AG	KarstadtQuelle Versicherung, Elvia, Die Bahn, Expedia.de, Otto
Price	400–10'000 (2002)	4,000–8,000 Euro (2001)
Annual fee	160–2'400	?
Recertification costs	?	80%

Remark: S@fer Shopping encompasses more than data privacy – it makes statements about the Internet shopping procedure of companies.

Excercise 4:

Describe a privacy-related issue that has been in the news recently. Which of the eight OECD principles got violated?

Solution:

Krankenkassen erfahren viel zu viel
Tages-Anzeiger vom 03.03.2009

Krankenkassen und Spitäler unterlaufen mit dem Einsatz von sogenannten Fallmanagern systematisch das Arztgeheimnis. Der Datenschützer hat diese rechtswidrige Praxis aufgedeckt.

Use Limitation: Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified under the preceding specification principle except (i) with the consent of the data subject, or (ii) by the authority of law.

In above case, medical data is disclosed to a third party (insurance company) without prior consent of the patient.