Mag. iur. Dr. techn. Michael Sonntag

Privacy

Institute for Information Processing and
Microprocessor Technology (FIM)
Johannes Kepler University Linz, Austria

E-Mail: sonntag@fim.uni-linz.ac.at
http://www.fim.uni-linz.ac.at/staff/sonntag.htm

Who is protected?

- EU directive: Only natural persons
  - → Austria: Extended to legal persons
- The intention is to protect humans from everything/-one else
  - → This includes:
    - » Children in relation to their parents
    - » Employees in relation to their manager/the employing company
    - » The managers from the public
  - → Excluded are:
    - » Anonymous persons
    - » Unique things
      - – Only as long as they are not associated with a single person!
- Legal entities are often protected only to a lesser degree
  - → See e.g. publishing financial data; or environmental pollution
  - → **They are included** in the (later) directive on privacy and electronic communications!

Identifiability

- Only persons identified or identifiable are protected
  - → If nobody can say who the person is the data relates to, there is no danger at all (purely statistical data)
  - → For the EU directive "nobody" means:
    - » Identification only through an external entity with no obligation to provide the information, like an ISP → Not identifiable
      - – Problem: The ISP itself? The police where the ISP must disclose it?
    - » Identification possible through own databases, from sources that are controlled, or where disclosure is obligatory → Identifiable
  - → Legally enforceable or practically possible → Identifiable
- Identification can be possible directly or indirectly
  - → E.g. one/more factors specific to physical, physiological, mental, economic, cultural, social identity
    - » "The blonde girl working in the accounting department"
    - » If there is only one a) young woman, with b) blond hair, c) in that department → Still identifiable

What is protected?

- All data relating to a protected person
  - → Example: Hair colour, voice, letters, personal habits or preferences, income, sexual orientation, last breakfast meal, creditworthiness, …
  - → Regardless whether it is "important“/”public” or not
    - » Together with other data it might become important
    - » Everyone can determine the importance for them autonomously
- Result: If there is a list of "person" (identified somehow) and "attribute(s) of this person", the list is protected!
  - → Note: There is one additional data hidden here: Being on the list!
  - → Example: List of name and address
    - » Public data (taken from phone book)
      - – Practically unprotected and completely harmless
    - » Add the heading: "AIDS patients"
      - – Suddenly this list becomes much more dangerous!

What is protected?

- Special protection exists for more "dangerous" data:
  - → "Sensitive" data: Closed list
    - » Racial/ethnic origin, political opinion, religious/philosophical beliefs, trade-union membership, health, sex life
  - → "Criminal" data: Closed list
    - » Offences, criminal convictions, security measures
      - – Does NOT refer to administrative sanctions or judgements in civil cases (national law may include them, however!)
  - → These two areas are more strongly restricted, but numerous exceptions are still possible (see later)
    - » Requirement for laws introducing exceptions:
      - – Normal data: "public interest"
      - – Sensitive data: "substantial public interest"
- "Closed list": Only what is listed and nothing else
  - → "Standard" protection: Everything (no closed list!)

What is protected?

- Only data that is processed
  - → Gathered, related to other, transformed, transferred, …
  - → But **NOT** the data as such ("Facts are free")!
    - » There is no restriction on hair colors, only on gathering, sorting, storing, adding to other data, etc. when connected to persons!
- “Public” data might still be protected!
  - → Especially if known only to a restricted public
- Data must be either
  - → automatically processed, or
    - » Computer systems in any form
  - → contained (or intended to be contained) in a filing system
    - » Criteria related to individuals necessary (see next slide!)
    - » Unimportant: local or distributed / functionally or geographically
    - » E.g. Database, filing cabinet with index

Exclusions from protection

- Some data/persons is excluded wholly from the applicability of the directive
  - → Matters outside the scope of the EU
    - » Excluded from the applicability in Austria in the law
- Not applicable in all points:
  - → No information, no objection, no supervision, …
  - → Areas:
    - » National/Public security: Police
    - » Defence: Military secret service
    - » State security, including the economic well-being of the state
      - – Includes the EU
      - – Examples: Secret service (terrorism; economic warfare)
    - » State activities in criminal law: Preventive measures
  - → Note: The ECHR still applies, i.e. all exclusions must still conform to it!

What is "data processing"?

- Processing is an all-encompassing term
  - → Includes any kind of operation on it
  - → Regardless whether automatic or manual!
    - » Usually there are significantly less restrictions for manual files
  - → Examples:
    - » Collecting: Obtaining personal data in the first place is already "processing" (noting at the skin colour of a person)
    - » Recording: Videotaping a person
    - » Storage: Copying the data somewhere
    - » Adaptation/alteration: Cutting the tape, changing brightness, …
    - » Retrieval: Looking up the skin colour of a person in a tape library
    - » Publication: Putting the video up on YouTube
    - » Combination: Adding the skin colour to the customer database
    - » Erasure: Destroying the tape and all copies (notes, …)
  - → Whatever you do with personal data, it is processing
    - » And therefore subject to the directive unless excluded/permitted!

Controller vs. Processor

- Controller: Any person which alone or jointly determines the purpose of data and the means for its processing
  - » This include natural and legal persons, states, …
  - → The person deciding what to collect and what to do with it
- Processor: Any person (natural, legal, state, …) actually performing the processing of data on behalf of a controller
  - → This person did not decide on what to do, they merely act
  - → "Performing the manual acts of processing"
- Example: Sending a paper mass mailing
  - → Controller: Owns the addresses and decides to send a letter with certain content to all of them
  - → Processor: Printshop receiving the addresses, printing them on envelopes, carrying them to the post office
    - » The post office is a processor too!

Confidentiality obligations

- Anyone acting under the authority of the controller or of the processor, including the processor himself, may only process personal data according to the instructions from the controller (or when required by law)
  - → This ensures that the controller is legally responsible for (almost) every processing with his data
    - » If someone does something clearly illegal and not required, this is their own fault then (→ they become the controller)!
  - → Ensures that data is not misused by processors
- Typically requires also a contract clause for all employees
  - → "Personal data will only be processed according to the directions given and not be disclosed to third persons"
  - → Important: Personal knowledge is often unavoidable → This must be restricted (if possible: chatting!)

Rights of the data subject

- The data subject has several rights
  - → Information, Access, Objecting (two different versions)
- Cannot be removed through contracts or terms of business
- Obligation of the data controller to enable them
  - → He need not provide incentives to do it
  - → He just isn't allowed to make it more difficult than necessary
- The data subject is obliged to cooperate
  - → Like providing the internal number of the processor if available to him ("customer number", …)
  - → Provide proof of identity
    - » Not: Using the right of access to get data on your neighbour …
- Restrictions are possible: National security etc.
  - → No access to your data in the police/secret service records!
  - → Correcting: Response is always the same “Was checked.”

Rights of the data subject: Information

- When collecting data, the following information must be provided to the data subject
  - » If the person doesn't have the information already
  - → Identity of the controller: Who am I?
  - → Purpose of the processing: What is intended
    - » Main reason: So the controller cannot use solely internal documentation of the purpose, which could be changed at a later point in time arbitrarily!
  - → Any further information required to fulfil the fairness principle
    - » (Categories of) recipients of the data
    - » Whether answering is obligatory and what the consequences are of not answering
      - – E.g. "Lottery ticket must be filled out completely or it is void"
    - » Existence of the right of access/correction
- See also "consent" above!

Rights of the data subject: Access

- The data subject has the right to request from the controller
  - → Whether data about him is being processed
  - → The purpose of the processing
  - → The categories of data processed (“column headings")
  - → The data on him being processed ("line content")
    - » In an intelligible form: I.e. codes must be explained
      - – Not just "customer class: 7a"!
  - → (Categories) of recipients of his data
  - → Source of the data on him, if available
- Rectification/erasure/blocking of unlawfully processed data
  - → Incomplete, inaccurate, …
  - → Type depends on the rights/interests of the processor
  - → Includes notification of recipients of data correct/deleted/…
    - » Unless impossible or it would require a disproportionate effort
- At reasonable intervals, without excessive delay/expense

Rights of the data subject: Objecting (1)

- In certain cases, if processing is allowed, the data subject still has the right to object (i.e. opt-out)
  - → When: Processing for public interest, legitimate interests
  - → When not: Processing because of national laws
  - → Requirement for objection is a compelling legitimate ground relating to the particular situation of the data subject
- Translation: In general you may process the data, but a few persons have distinct and special reasons to be excluded!
  - → You have to explain why the general weighing of interests in your specific case is tipped in the other direction than for all other (=“normal”) persons, for which this is no problem!

Rights of the data subject: Objecting (2)

- If the data is (to be) used for direct marketing
  - → Like sending out advertisements
- The data subject can object to this
  - → On request: Opt-out, not opt-in
  - → Process must be free of charge!
    - » OK: Fax, Webpage, E-Mail, Letter
    - » Not: Added-price telephone numbers
- Must be expressly offered this right
  - → See small print on competition cards: "I consent to the storage and processing of my data in IT systems and consent to its use for advertisement purposes. This consent can be withdrawn at any time."

Security of processing

- Controller must secure the data
  - → against accidental or unlawful destruction, loss or alteration
    - » Unmodified existence of data must be ensured “Security”
  - → against unauthorized disclosure or access
    - » Confidentiality of the data “Protection”
- by appropriate
  - → technical and organizational measures: See next slide!
- The controller is responsible for both; he must transfer these requirements to any processor he employs
  - → Requires a binding legal act containing that the
    - » processor may act only on instructions by the controller
    - » processor must fulfil all necessary (see later) security measures
  - → Act must be in writing or in an equivalent form

Security of processing: Level of protection

- According to the state of the art
  - → New technologies: Must be considered immediately!
  - → Not: State of science (=much higher!)
- According to the cost of their implementation
  - → Not everything possible is mandatory!
- Security level must match the risks represented by the processing and the nature of the data
  - → Depends on a general view: How "dangerous" disclosure, deletion, … of such data is for the "typical" data subject
    - » If single persons are in more danger → not considered!
  - → Danger = Danger to subject, not to processor!
- Result: Asses the data and the risks, review the methods to secure them with their costs, and then select and implement a matching level of protection

Notification

- Before any kind of automatic processing of personal data is allowed, the public authority must be notified of it
  - → A bit problematic in practice, so several exceptions exists!
- Basic idea: Public register + checking the lawfulness
  - → Prior checking for "dangerous" kinds of processing
- Simplification/Exemption:
  - → Public register instituted by law with open access
  - → Internal processing of political, philosophical, religious or trade-union aim
  - → Manual processing (may be included by countries)
  - → Ensuring that the rights of data subjects are unlikely to be affected adversely, by instituting a personal data protection officer according to national law responsible for independently ensuring the protection of the data and keeping a processing register for this controller

Notification: General exemptions

- General exemptions are possible when adverse effects for the data subject are unlikely because of the data processed
- They must specify
  - → Purpose of processing
  - → Data categories: What data will be stored & processed
  - → Categories of data subjects: Whose data will be processed
    - » Not by name, but as a general description
  - → Categories of recipients of the data
    - » Who will receive the data (or which subset of it); can be "none"
  - → Length of time of storage: Limitation of the purpose
- Generally most important and common kinds of processing are exempted
  - → Examples: Accounting, direct mailings, employee/user lists …

Content of notification

- Minimum content of notifications:
  - → Name + address of the controller
    - » And its representative (companies!)
  - → Purpose of processing
    - » Length of time of storage results from this purpose
  - → Categories of
    - » Data
    - » Data subjects
    - » Data recipients
  - → Proposed transfers to third countries
    - » Such notifications will usually be investigated in detail!
  - → General description of security measures
    - » Detailed enough to allow verification of lawfulness
- Changes in any element must be notified as well

Public register of processing operations

- All processing operations of personal data must be public
  - → Fact that, and what categories for what purpose in which way
- This is done by a public register of all data processing
  - → Handled by the supervisory authority
- What about the exemptions?
  - → The controllers (or someone else → national law) must make the information available to any person on request
    - » This means, everyone can ask any company/person/… whether it processes personal data and the details about it
    - » This does not require that data on this person is handled!
  - → Excluded: Public registers instituted by law with public access
- Any person may inspect this register

Transfer of data to third countries

- Transfer of data to third countries is only allowed if an adequate level of protection exists there
- Adequacy: All circumstances surrounding the transfer, esp.
  - → Nature of the data transferred
  - → Purpose and duration of processing
    - » I.e. "Export" or only a short "remote processing"
  - → Country of original and final destination country
  - → Laws, professional rules & security measures in third country
- Commission may decide, which countries possess such an adequate level of protection
  - → Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay
  - → USA, Australia: Passenger Name Records
  - → USA: Safe Harbour
    - » NOT the USA in general!

Transfer of data to third countries

- Other possibilities (i.e. no Safe Harbour/exclusion needed):
  - → Special contractual clauses (see model contracts later!)
  - → data subject has unambiguously given consent
  - → necessary for performance of a contract between data subject & controller or implementation of precontractual measures taken in response to data subject's request
  - → necessary for conclusion/performance of contract concluded in interest of data subject between controller and third party
  - → necessary or legally required by important public interest, or for the establishment, exercise or defence of legal claims
  - → necessary in order to protect vital interests of data subject
  - → transfer is made from a register based on law, intended to provide information to public, open to consultation by public in general or any person demonstrating legitimate interest, and only to the extent that the conditions laid down in law for consultation are fulfilled in the particular case

"Safe Harbor"

- Problem of large international companies:
  - → Customer data is stored on central servers in the USA
    - » Good reasons for central storage according to computer science!
  - → This is an export from the EU
    - » Although it will be "re-imported" for fulfilling contracts
  - → Once outside, it could be reused for any purpose whatsoever!
- Separate datacenter is expensive and difficult
  - → A kind of "model contract" specifically for the USA
  - → If accepted, there exists and adequate level of data protection within this single company
  - → Onward transfer: Data may not leave the protected "harbor"!
- Enforcement through the Federal Trade Commission or the Department of Transportation
  - → Investigation of complaints, but includes awarding damages

„Safe Harbor“ Basics (1)

- Seven basic principles, that are required
  - → Notice: Information on data collected and its purpose, how to contact the organization, third parties data is diclosed to, …
    - » Privacy policy stating what is to be gathered and the purpose
    - » Very important: Only enforceable what is in there!
  - → Choice: Opting-out of collection and transfer to third parties and transmission (=change of purpose)
  - → Onward Transfer: Must remain within Safe Harbor
    - » Or back to the EU or model contract
  - → Security: Similar security requirements as in EU
    - » Reasonable precautions against loss, misuse, unauthorized access, disclosure, alteration and destruction
  - → Data Integrity: Data must be relevant & reliable for purpose
    - » For intended use only: accurate, complete and current
    - » See principles! Minimalism is not in here, however …

„Safe Harbor“ Basics (2)

- Seven basic principles, that are required (cont.)
  - → Access: Data subject has rights of access, correction, and deletion if inaccurate (some exclusion apply)
  - → Enforcement: Effective means for enforcement
    - » Minimum:
      - – Readily available & affordable independent recourse mechanism
      - – Follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented
      - – Adherence to attestations, assertions, and principles and consequences (sanctions) for non-compliance
    - » Typically some kind of alternate dispute resolution (arbitration)
- Certification: Can be external, but typically self-certified
  - → Must be done every 12 month

Safe Harbor: Problems

- Study (2008) found several problems:
  - » http://www.galexia.com/public/research/articles/research_articles-pa08.html
  - → 206 companies claimed to be part of it, but were not
    - » Only one (1!) company was convicted (but not fined!)
    - » Several of them also used trust seals without authorization
  - → Merely 384 companies are really part of safe harbor as they fulfil the most basic principles (e.g. having a privacy policy)
    - » Only one principle (of 7; enforcement & dispute resolution) was checked here!
  - → 209 companies selected very expensive arbitration providers
    - » Minimum costs: US$ 120-1200/hour; 4 hours minimum, US$ 950 administrative fee
    - » Costs are not disclosed or must be shared by the consumer
- No certification or evaluation of the members
  - → You claim to fulfil everything, that's it!
    - » You must pay fees: US$ 200 for registration, US$ 100/year

"Model contracts“ I

- For the transfer of personal data to third countries without an appropriate level of protection, this level can be created by adding clauses into the contract with the recipient
  - → This is quite difficult, so model contracts have been drawn up
  - → Then data can be exported everywhere!
- Two sets currently exist in parallel
  - → Mixing is not allowed, however!
  - → Additional (non-contravening) clauses possible
    - » Example: Business elements (what to do how, …); Indemnification, dispute resolution between exporter and importer, cost allocation, additional termination clauses, …
- Important principles contained:
  - → Purpose limitation; data quality and proportionality; transparency; security and confidentiality; rights of access, rectification, deletion and objection; sensitive data; marketing data; automated decisions;

"Model contracts“ II

- Standard clauses for mere processing outside of the EU
  - → This means, no transmission takes place, just the physical act is performed outside of the EU
- Basic model: EEA Controller → Non-EEA Processor → Non-EEA Subprocessor: Clauses apply to the last step only!
  - → First step: Similar clauses, but not these!
    - » No standard clauses exist there; these might be “reused” in slightly modified form
    - » Similar: EEA Processor → Non-EEA Subprocessor
  - → So these are perhaps not that useful?!?
- Data subject is a third-party beneficiary to the contract
  - → An uncommon construct, but the only thing work here!
- Contract must be signed separately for each data exporter
  - → Because the data exporter, the subjects, data categories etc. are all part of the contract and will be different

"Model contracts“ II

- Selected content:
  - → Data may be processed only according to the directions of the exporter of the data
  - → Importer must guarantee sufficient technical and organisation security measures and ensures compliance
  - → On request the contract + a summary description of the security measures must be disclosed to the data subject
    - » Commercial information may be removed
  - → Further subprocessing must pass on the clauses in writing
  - → Liability: Compensation by exporter (subsidiary only: importer)
  - → Mediation is mandatory when requested by data subject
  - → Governing law: Law of the data exporter
  - → Copy of contract must be deposited at DP Authority
    - » DPA also may perform audits at importer and subprocessor!

Conclusions

- Privacy is an important aspect in a free society
  - → Diverging interests must be balanced
- Currently privacy in on a constant decline
  - → Fear of terrorism
  - → "I have nothing to hide"
- Privacy legislation is quite strict and very effective in theory
  - → In practice it is often ignored to a large degree
  - → Only seldom infractions become known and are prosecuted
- Problematic are especially the security precautions
  - → Illegally selling data is rather rare, as far as known
  - → Illegally obtaining data (hacking) or losing it is common!
    - » Stolen laptops, unencrypted backup tapes lost, …

Questions?

Thank you for your attention!