Mag. iur. Dr. techn. Michael Sonntag

# Privacy

## Rechtsgrundlagen für Informatiker

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

# Agenda

- What is privacy?
  - → The basic right
  - → Giving "consent"
  - → Exclusions
- The EU privacy directive
  - → Who is protected?
  - → What is protected?
  - → When is data processing allowed?
  - → Obligatory security precautions
  - → Rights of the data subject
  - → Transfer to third countries
  - → Enforcement, remedies, liability

# Introduction: Why privacy?

- "Why privacy? I don't have anything to conceal!"
  - → In theory, yes, but actually….
    - » See film stars: Every photo of a private activity will be published
      - – Whether it is scratching your nose or kissing someone
  - → Harmless activity can easily be misunderstood or misused!
- A constant thought of "I'm being watched…" builds up
  - → Psychologically this produces constant pressure and a general fear
    - – "I don't trust you, because you are being watched!"
    - » This breeds conformity and prevents any kind of open discussion etc. if taken too far
    - » Example: Who will discuss politics if every word is recorded, stored, and later perhaps used against you?
      - – Therefore politicians always contradict themselves!
- Constant supervision treats humans as objects
  - → Reversal of "innocent until proved"

# Why the need for personal data?

- Large, but unfocused, desire for privacy by individuals
  - → "The right to be left alone" (Warren/Brandeis, 1890)
    - » Today extended: To self-determine information about you
    - » From passive ("don't talk about me") to active ("You have to guard the information about me")
  - → Privacy is usually not important, unless concrete personal drawbacks are experienced
- Large desire for information by companies
  - → Know your customers, advertising, credit rating, …
    - » Key word: "Personalisation" → Talk to the customer as an individual (or member of a certain group) instead of as a generic human being
      - – Small local store → supermarket → combination of both

**Some balance must be found!**

# Dangers of a missing balance

- Otherwise there will be:
  - → The danger of secretly gathering data
    - » See the discussion about hidden online searches!
  - → The danger of exchanging and correlating data uncontrolled
    - » Fusion of Google and DoubleClick
      - – Google has search results, DoubleClick the personal information, ...
  - → No advantages of personalization
    - » Amazon is successful because of such features
  - → No advantages of not requiring standard information
    - » Everyone complains about having to provide the same certificates again and again to the administration
  - → Secret classification
    - » You won't get a mobile phone, but nobody would tell you why
      - – So you can't contest this decision or change the basic facts
  - → …

# Data: Protection / Security / Privacy / … ?

- Terminology is important here!
- Data Protection: Protection against disclosure
  - → Data should be kept secret
  - → (Data) Privacy = Data Protection
    - » Note: Generally, this would be data "security"!
      - – Preventing unauthorized access
  - → German: "Datenschutz"
- Data Security: Protection against loss
  - → Data should be available (to the subject and the owner)
  - → German: "Datensicherheit"
- Both aspects are important
  - → Here only the first one is discussed!

# Privacy vs. terrorism

- But in some cases monitoring is necessary
  - → This has already been acknowledged by privacy laws
  - → The important discussion is: Where to draw the line!
- Terrorism is a very "public" crime: Although the number of people dying by it in western countries is negligible compared to car accidents, it is an excellent "reason"
  - → Nobody fears being hit by a car,
  - → but (almost) everyone is in panic of bombs!
- Terrorism is a problem, as "modern" terrorism is almost impossible to stop by surveillance. It only helps afterwards to identify terrorists and perhaps some of their associates
  - → This is still important, but one step less than prevention
  - → This area is currently hotly disputed, and politics (not necessarily the police!) request lots of additional options

# The basic right to privacy

- The right to privacy is "the right to be let alone"
  - → Not everything a person does may be observed, noted, used, stored, calculated with etc.
  - → Today seen more extensive: That a person may decide what is known about him/her by others
- This includes the prohibition to obtain personal data!
  - → The problem is not necessarily what happens with the data, but that data exists at all: It might be (un-)intentionally disclosed; and if data exists it will be used sometimes!
    - » See the highway toll in Germany as an example
- Sometimes personal data is "known" inevitably
  - → Example: Doctor's secretaries/aides
  - → Then privacy refers to the prohibition to disclose the information to third persons or use it for any other task

# The EU Privacy Directive

Directive 95/46/EC from 24.10.1995

# 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
    - » 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

# Identifiability: Pseudonyms

- Pseudonym:
  - → Partitioning data into an identifying part and a random number
    - » E.g.: Name, address, social security number, … + RND
  - → and other data + same random number
    - » Like surfing habits, credit rating, …+ RND
- Every person has access to only a single part
  - → One employee knows all about person number 4711
  - → Another employee knows, who person number 4711 is
    - » But no other fact about this person!
- Still personally identifiable data, but much more secure!
  - → At least two persons are required for compromising data
- Difficulty: Partitioning!
  - → The "other data" might in total already be sufficient to again identify the person!

# 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" 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, 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.!
- "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
    - » Unimportant: local or distributed / functionally or geographically
    - » E.g. Database, filing cabinet with index

# What is not protected?

- Unordered collections
  - → Intended for the administration: Large archives
- When there is at least one criteria for searching the content easily (not just serial exhaustive search), it is protected!
  - → Administration archives: In paper form only searchable by case number → This is not really dangerous and excluded
    - » Reading through every single case to find the desired data is not really workable
  - → As soon as there exists an index of persons and the case numbers they occur in, this is a protected collection
    - » Note: Electronic archives will always be protected, as there a full text search is always possible easily!

# 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
    - » State activities in criminal law: Preventive measures
  - → Note: The ECHR still applies, i.e. exclusions must also conform to it!

# Personal usage

- Purely personal or household activity by a natural person
- Examples:
  - → Personal telephone directory
  - → List of your friend's birthdays
- Usually there exists a further restriction:
  - → This data may not leave the personal area
  - → Gathering the data is only allowed with the consent of the data subject or from public data
- This is a restrictive exclusion: Public discussion (gazettes) of personal matters (celebrities!) doesn't match this exclusion!

# Exclusions: Overview

- The basic right prohibits any use of personal data
  - → See above: This will not work in society
- Several exclusions exist, when personal data may be collected, used, stored etc.
  - → Typically, transferring the data is much more restricted!
  - → Fewer exclusions exist for the more "dangerous" subsets of data: sensitive and criminal data
- In the EU directive the exclusions are very general
  - → National law can either define them in more detail, like in Austria, or leave it up to the courts
- In general, there is a weighing of interests between the person the data is about, and the person wanting to use it
  - → Some decisions of this weighing has been included in the directive as a pre-determined result!

# Normal data may only be processed if (1)

- the subject has unambiguously given consent
  - → See definition of consent later!
    - » "Unambiguous" → Implied consent is possible here
  - → Everyone can do with his data as he wants
    - » The freedom not to use the protection of the law
    - » See e.g. television talkshows!
- it is necessary for the performance of a contract
  - → Data subject must be party to contract, or
  - → for taking steps at request of subject prior to contract
    - » E. g. checking creditworthiness, calculating shipping costs, …
  - → Otherwise this could be used as a right of withdrawal!
    - » If later you do not want the contract any more and prohibit the seller to use your address ⇒ He couldn't ship the goods!

# Normal data may only be processed if (2)

- it is necessary for compliance with a legal obligation
  - → Obligation of the controller, i.e. the one processing the data!
  - → Examples: Archiving invoices, processing data of the employee by the employer (holidays, payment, ...)
- it is necessary to protect vital interests of the subject
  - → E.g. looking up her own blood group on serious injuries
  - → "Vital" must be seen narrowly
    - » "Of interest" or "possibly beneficial" is not enough!
- it is necessary for tasks of public interest/official authority
  - → To avoid having to explicitly grant all processing by law
  - → Must be an important or indispensable requirement, not just a reduction of work
- it is necessary for legitimate interests of the controller, third parties, or those to whom data is disclosed
  - → **EXCEPT** where the interests of the subject are stronger!

# "Consent" in the context of privacy

- Must be "informed consent"
- This includes three aspects:
  - → Must be given freely ("Freedom")
  - → Must be specific ("Specificity")
  - → Subject must be informed ("Information")
- Can be given explicitly or implied
  - → What is needed depends on the category of data
    - » "Normal" data: Implied consent sufficient
    - » "Sensitive" data: Consent must be given explicitly
  - → Usually there is no need for consent in "writing"
    - » At least not in the EU directive
    - » Germany previously required "written consent", which was a problem in the Internet, although el. signatures did exist then
      - – But nobody used them, so this was abolished!

# Freedom

- No duress or compulsion
  - → Denial of contract (if not unethical) possible if not given!
    - » BUT: Effective monopolies; e.g. all banks do it???
    - » In practice quite a lot is possible under such a condition
- But these are necessary conditions for every legal act?!?
  - → Then there must be a bit more freedom here!
- One typical example are work contracts
  - → In the contract usually quite a lot of conditions can be added
    - » Everyone is free to accept this contract or decline
      - – Which is perhaps not that true in practice….
  - → But for an employee there is almost no possibility to give valid consent to his employer later!
    - » "You **will** allow this or I'll **sack** you!"…

# Information

- Information necessary on
  - → That some personal data is used
    - » "We will collect, store, …. your personal data …"
  - → What data is used
    - » "We collect your IP address, web sites visited, and all information on the forms filled in"
  - → Who is the person using it
    - » "We are the ACME Inc."
  - → Whom it will be transferred to (if applicable)
    - » NOT “to everybody we want to”
- Especially important for implied consent
  - → Consent is only possible to the things actually disclosed!

# Specificity

- Consent cannot be given for unlimited applications
  - → Only (a list of) single applications, but not a "general" consent
- Specificity means:
  - → For a certain purpose: A closed list/described set
    - » **NOT** “we are allowed to do with it what we want”
    - » This is the most important part!
      - – Example: "Advertisements" is not specific enough
    - » However, no absolutely closed list is required
      - – "Marketing our own products" could be sufficient
  - → For a certain controller
    - » **NOT** “we may transfer it to everyone we like”
  - → Of certain data
    - » **NOT** "whatever we know or find out about you"

# Weighing the interests

- **Weighing of interests required**
  - → This is an "opening clause": You may do whatever you want with any "normal" personal data, but you need to have:
    - » Some interests: Easy!
    - » They must be legitimate: Usually no problem!
    - » They must outweigh the interest of the person to keep the data private: Most important and typically difficult aspect!
  - → Examples:
    - » Vital interests of thirds: Searching DBs to find suitable blood donors
      - – To contact them to ask, whether they would be willing to donate blood
    - » Required for pursuing a claim before public authorities
    - » Cooperation through official channels to improve public admin.
  - → May **not** be **just** a monetary comparison
    - » Gain for processor vs. damage to subject → Always insufficient!
  - → General clause for all other uses!

# Sensitive data may only be processed if (1)

- the data subject has given explicit consent
  - → Countries can define some areas, where even consent is not enough, i.e. where the person is protected from itself!
- processing is necessary for carrying out obligations/specific rights of the controller in employment law
  - → If this is authorized by national law
  - → Adequate safeguards must be ensured
  - → Example: Accounting includes health information
    - » AT: Trade-union membership fee is partly collected by employer!
- processing is necessary to protect the vital interests of the subject or another person
  - → Only if subject is physically/legally incapable of giving consent
    - » Otherwise: The subject must be asked!
  - → No denying possible regarding vital interests of others!

# Sensitive data may only be processed if (2)

- processing occurs by a foundation, association, … with a political, philosophical, religious or trade-union aim for their members or persons with regular contact connected with their purpose
  - → I.e., churches may have lists of members and supporters
  - → Only for legitimate activities and with appropriate guarantees
  - → This data may not be disclosed to thirds without consent!
- the processing of data manifestly made public by the subject
  - → After a "coming-out" the sexual orientation may be stored
- the processing is necessary for the establishment, exercise or defense of legal claims
  - → You may use personal data in courts to prove your case

# Sensitive data may only be processed if (3)

- the processing regards preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services
  - → Data must be processed by a health professional with an obligation of professional secrecy (or persons with equivalent obligation of secrecy)
- Other national legal exemptions with suitable safeguards are possible for reasons of substantial public interest
  - → Examples: Private use, scientific research, statistics, informing the data subject, catastrophes etc.

# Which countries law's are applicable?

- Each country regulates data processing within its boundary
  - → An establishment on its territory, where data is processed
    - » Multinational company: National law applies to each establishment separately, i.e. where it is physically located
    - » This does not depend on where the data logically belongs to!
      - – Usual delineation: Processing in a country without establishment Law from the country where the main seat is located applies
  - → An establishment outside the EU where international law dictates, that the law of this EU country is to be applied
  - → Established solely outside the EU but processing takes place on equipment within the EU
- Exclusion from applicability: Mere transfer
  - → Transporting data through the EU is excluded
    - » Any kind of "working" on or with it → EU law applies
  - → Example: Data sent from USA to China via Internet through London

# 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" (looking 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
  - → Whatever you do with personal data, its 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 processing data on behalf of a controller
  - → This person did not decide on what to do
  - → "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 makes sure, 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!
  - → 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!)

# Principles for data quality

- Several general principles exist, which must be heeded in the national laws
  - → They are also important for the interpretation of these laws
  - → The controller of data is responsible for ensuring that there are observed fully
- But in general the laws should be sufficient!

- Fair and lawful processing
  - → The second part hasn't much meaning …
  - → But the first is important:
    - » The interests of the data subject and the data owner must be balanced; both monetary and non-monetary
    - » Especially regarding its purpose: It must be disclosed correctly, understandably, not changed afterwards, …
    - » See also later: Information requirements

# Principles for data quality: Specific purpose

- Collection is only allowed for a specified, explicit and legitimate purpose
  - → But this can be set arbitrarily
  - → Must be done before any collection!
- This means, any later change in the purpose is forbidden!
  - → Unless a legal exception exists!
  - → Otherwise: Collect data for own advertising purpose, and then sell it to credit rating companies, sex magazines, …
- Change of purpose = Transmission
  - → Usually much more tightly regulated than processing
  - → Transmission can take place within a company: Changing the "label" of the data, i.e. its purpose, is a transmission
- Exceptions for history, research, statistics is possible (transfer!), but requires additional safeguards in the law

# Principles for data quality: Adequacy

- Data must be adequate, relevant and not excessive in relation to the purpose and for further processing
- Adequate:
  - → You must collect data which is sufficient for the purpose
    - » Otherwise it doesn't make sense and the real purpose is probably something different
      - – Some data values might always be insufficient/incomplete/…
- Relevant and not excessive: Minimalism principle
  - → You may only collect what is actually needed for the purpose
    - » No collecting "just in case", "a bit around the edges", …
  - → Note: The purpose can be set very wide…
    - » Example: "Data on unpaid invoices"
      - – When paid → Would have to be removed from the database
      - – Better: "Data on delayed payments"
    - » Modifying the purpose later is difficult!

# Principles for data quality: Accurate and up-to-date

- Data must be accurate and up-to-date
  - → This is relativized: Only regarding the purpose!
- Accurate: The data must be complete and correct
  - → Example: Collecting "date of birth"
    - » The year might be sufficient: Checking an age limit
    - » The full date might be required: Looking up in official databases
- Up-to-date: The data must continuously be monitored, checked, and updated
  - → If its important data, this actually means proactive checking!
    - » Then also informing all previous recipients is necessary
    - » Example: Credit rating
  - → Generally, there is no obligation to do anything
    - » If you notice, e.g. through a complaint by the data subject, that there is a mistake, you must then correct it
  - → Sometimes the correctness is not clear: Annotation or deletion might be in order

# Principles for data quality: Only as long as needed

- If the purpose is fulfilled, the data must be deleted
  - → Actually, anonymization is sufficient as the data is then no longer personal data
    - » Pseudonymization is insufficient, however!
- Depends largely on the definition of the purpose
  - → In practice, the purpose is set wide so that data may be retained almost indefinitely
    - » But see discussion on retention duration of search engine logs!
- Theoretically, this would mean also deleting all the data from backup tapes, leaving only the rest of the backup
  - → This is impractical and seen as not necessarily required
    - » But it must be deleted after restoring from the backup!

# Rights of the data subject

- The data subject has several rights
  - → Information, Access, Objecting (two different instances)
- Cannot be removed through contracts or terms of business
- Obligation of the data controller to enable this
  - → 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 with the processor if available to him ("customer number", …)
  - → Provide proof of identity
    - » Employing the right of access to get data on your neighbour…
- Restrictions are possible: National security, …
  - → No access to your data in the police/secret service records!

# 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 ("table 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 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 has the right to object (i.e., opt-out)
  - → When: Processing for public interest, legitimate interests
  - → And not: Processing because of national laws
  - → Required: Compelling legitimate grounds relating to his particular situation
- 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 case is tipped in the other direction

# 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
  - → 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."

# Automated individual decisions

- Everybody has the right not to be the subject of an solely automated decision with legal effects
- If the processing is intended to evaluate certain personal aspects relating to him
  - → Therefore doesn't apply to processing addresses for advertisement: The addressee is not "evaluated" there
- Examples:
  - → Work performance, creditworthiness, reliability, conduct, …
- Exceptions:
  - → Authorization by a law with safeguards
  - → Entering/performance of a contract and this is approved
    - » I.e., fully automated creditworthiness check is allowed, if the end result is positive and the application is accepted
  - → Suitable measures available to safeguard legitimate interests
    - » Example: **Allowing the data subject to comment on it**

# Security of processing

- Controller must secure the data
  - → against accidental or unlawful destruction, loss or alteration
    - » Unmodified existence of data must be ensured
  - → against unauthorized disclosure or access
    - » Confidentiality of the data
- by appropriate
  - → technical and organizational measures: See next slide!
- Controller is responsible; must transfer these requirements to any processor he employs
  - → Requires a binding legal act containing
    - » 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: Typical minimal measures

- The minimum level of protection includes:
  - → This is independent of the value/danger of the data
    - » But the extent of these measures depends on it!
  - → Explicit rules who may do what with personal data
  - → Employment contract:
    - » Processing only according to valid commands
    - » Information on the obligation of secrecy
    - » How is allowed to use which systems
  - → Access to rooms with personal data must be regulated
  - → Media with personal data must be secured
  - → Protocols on any step of processing
    - » Examples of the different levels
      - – Addresses for marketing → On file/database level
      - – Medical data → Each read and write access to a single field
  - → Documentation on all security measures taken

# Security of processing: Typical minimal measures

- To consider technically:
  - → Encryption: On all transfers over public networks
    - » E.g. SSL: Credit card companies require it when accepting credit card online (no contract with them otherwise)
  - → Partitioning (pseudonyms): Wherever possible
  - → Access rights: Necessary for every single bit of personal data
    - » Includes secure user identification
  - → Personal data on a separate and separately secured server
    - » Web servers are notoriously broken into → sep. database sever
  - → Configurable logging facilities
  - → Storage of text and date/time of consents
    - » To be able to prove the person gave consent later!
  - → Special focus on backups: Encrypted/secure storage
    - » The security level must apply to all copies identically

# Security of processing: Level of protection

- According to the state of the art
  - → New technologies: Must be considered immediately!
- 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!
- 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

# Supervision

- Every state must have at least one supervisory authority
  - → Responsible for monitoring the implementation of the directive
- Must be completely independent
- To be consulted for laws/regulations affecting personal data
- May
  - → Investigate: Access all data processing systems
  - → Intervene: Orders, warnings, admonishments, …
  - → Start legal proceedings: Violations of laws pursuant to the dir.
    - » Appeal on decisions must be possible to courts
- Hearing claims by any person concerning the protection of their rights/freedoms regarding processing of personal data
  - → The person must be informed on the outcome of the claim
  - → Exemptions because of national security, …: Information, that a check was made (but not its outcome!)

# Notification

- Before any kind of automatic processing of personal data is allowed, it must be notified to the public authority
  - → 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, religiuous 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 more 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 the most important and common kinds of processing are exempted
  - → Typical 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
  - → Data categories
  - → Categories of data subjects
  - → Categories of recipients of the data
  - → Proposed transfers to third countries
    - » These will 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

# Remedies

- Administrative provisions are possible
  - → Optional
- Supervisory authority can start legal proceedings or act autonomously
  - → Independent → May do quite a lot without ECHR conflict!
- Judicial remedy must be possible for all rights
  - → Note, that in a member state this need not necessarily be a "court", but could be any kind of "tribunal"!
    - » Which must fulfil the following requirements
      - – Independent
      - – Impartial
      - – "Longer" appointment of judges
      - – Based on laws and with proper procedures
        - » Includes e.g. a public trial

# Liability

- Any person suffering damages as a result of unlawful processing of his/her personal data is entitled to compensation
  - → Must be paid by the controller
  - → If the act was performed by a processor, the controller might acquire compensation from him according to national law
    - » But this is a second and internal step!
- No compensation is due (wholly or partly) if the controller proves that he is not responsible
  - → The burden of proof is on the controller!
  - → Example: Completely autonomous act by a processor
    - » I.e., contrary to his contractual obligations/limits

# Sanctions

- Member states must impose sanctions for infringements of the laws adopted to implement the directive
  - → Reason: The EU has no competency for sanctions; these are completely national!
- Austria: Two kinds of sanctions
  - → When a requirement of the law has been breached
  - → When a breach of secrecy, etc. is more likely
    - » No security measures, …
    - » Sanctions already then, when no problem has (yet!) occurred

# 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
  - → Argentina, Canada, Switzerland, Guernsey, Isle of Man
  - → USA: Passenger Name Records, Safe Harbor
    - » NOT the USA in general!
- Other possibilities:
  - → Unambiguous consent, necessity for contract, …

# "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

# "Model contracts"

- 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 contract 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: 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;

# The "Art. 29 Data Protection Working party"

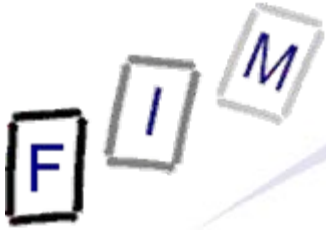
- Name stems from Art. 29 of the directive
  - → "Working Party on the Protection of Individuals with regard to the Processing of Personal Data"
    - » Also incorporated into the telecommunications privacy directive
- Members: Representatives of the supervisory authority of each member state + 2 representatives from the EU
- Tasks:
  - → Provide expert opinion to the commission on data protection
    - » Esp. regarding adequacy of data protection in third countries
  - → Promote uniform application of the directive in member states
  - → Advise the commission on measures affecting the processing of personal data and privacy
  - → Recommendation to the public, esp. community institutions, on matters relating to the protection of persons with regard to the processing of personal data and privacy in the community
    - » I.e. they may inform the press, ant not solely the commission!

# The "Art. 29 Working party"

- Produces a lot of documents and hints
  - → Note: Recommendations are often very relevant for business and provide detailed implementation hints
  - → But they are not binding as such!
    - » However, if they require certain elements, the national supervisory authorities will usually require the same…
- Work program for 2008-2009 (Internet related only!)
  - → Search engines (already issued)
  - → On-line social networks
  - → Behavioural profiling, data mining
  - → Digital broadcasting
  - → ICANN and WHOIS
- Work program (other): RFID, Biometrics, el. toll systems, PNR, SWIFT, eHealth patient records, …

# 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!**