Compliance and Operational Security
- Lecture -

Mirosław Kutyłowski

Department of Computer Science
Faculty of Fundamental Problems of Technology
Wrocław University of Science and Technology
POWER 2019

Fundusze Europejskie Wiedza Edukacja Rozwój
Politechnika Wrocławska
Unia Europejska Europejski Fundusz Społeczny
„ZPR PWr – Zintegrowany Program Rozwoju Politechniki Wrocławskiej”

Threats

Example I - smart meters

- communication scenario: a smart electricity meter communicates with a mobile reader or over a cellular network,
- smart grid: important data to be sent to the power grid: current usage (balancing power supply is a complex issue and these data may help a lot)
- confidentiality: communication in the plaintext, only MAC authentication in order to protect data integrity

The data seems to be harmless.
What is wrong about disclosing how much energy I use?

Threats

Wrong!

burglary optimization:

- big data collection: gather data from many smart meters, derive energy usage over time
- analyze data: surprisingly a lot can be learnt, learn how many people live in a house, when they are present at home, when sleep, when go for vacation
- burglary optimization: choose target according to risk optimization: nobody at home, nobody in the neighborhood
- optimize the operational costs: “travelling thief problem”

remarks:

- easy eavesdropping: mobile units (a small antenna in a car in a neighborhood), a big capture range
- other threats: kidnapping, stalking, terror, military intelligence, threats: “we know all about you”...

Threats

Tracing a credit card owner

old generation credit cards - no chip, magnetic strip only

- undeniability: no possibility to authenticate a transaction
- semipublic card number
- monitoring: card issuer traces activities and detects suspicious transactions – in case of detection such transactions blocked
- no technical barrier to create a clone of a card

Attack:

- gather data about owner's "standard behavior"
- perform a payment according to this standard pattern with a fake card
- $\Rightarrow$ monitoring fails to stop the transaction, no chance for complaints from the client

Attacks on ATM cards

against cards with a magnetic strip. The data on customer's behavior – from the bank's internal system.

GDPR Regulation

GDPR Regulation in EU

Legal concept

- Regulation: applies directly, no national law can overwrite it
- formerly Directive: required (obligatory) implementation in national laws.
  - inconsistencies between different implementations of the same Directive
  - necessity of comparing each pair of national regulations – high costs
  - harder for non-EU countries to adjust

Overview

1. preamble: describing goals, principles, situation. important for interpretation, easier to understand
2. articles: legal part (a formal specification)

Regulation scope

Territorial scope

1. the activities of an establishment in the Union, regardless of whether the processing takes place in EU or not.
2. processing data of data subjects who are in the Union by a controller or processor not established in the Union, related to:
   - the offering of goods or services (also for free) to colorblue data subjects in the EU
   - behavior monitoring as far as behavior taking place within the EU

Consequences

- applies to services such as Google for the customers in the EU
- profiling of the people in EU is within the scope
- problem of cookies (monitoring!)

Corollary: if a service is global, then better comply with GDPR right away!

Regulation scope

Material scope

applies to the processing of personal data wholly or partly by automated means

and

to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Consequences

- any ICT system means at least “partly by automated means”
- even if an IT system is fed with data gathered manually, then again the Regulation applies

Regulation scope

Material scope - exempts

Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;
(e.g.: military defense)

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
(common foreign and security policy)

(c) by a natural person in the course of a purely personal or household activity;
(private use)

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

GDPR legal notions

“Personal data”

any information relating to an identified or identifiable natural person (“data subject”);

an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Warning

much broader meaning than one could expect
RECOMMENDATION: apply pseudonymization or anonymization whenever possible

GDPR legal notions

“Processing”

any operation or set of operations

which is performed on personal data or on sets of personal data,

whether or not by automated means,

such as collection, recording, organization, structuring, storage,adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

corollary

- possessing personal data already means “processing”.
- destroying is also processing and must be lawful

GDPR legal notions

“Profiling”

any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person,
in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

corollary

within the scope of profiling:

- cookies
- recommendation systems
- . . .

GDPR legal notions

“Pseudonymization”

processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

corollary

pseudonymization reversible with additional keys

apply whenever it might be necessary to recover the link to a natural person

GDPR legal notions

"Pseudonymization"- example

all computations in a group of a prime order q with hard DHP:

- a user A holds a secret key x,
- an ID Authority holds the public keys of the users, the key for A is g^x
- for domain D there is a corresponding domain public key $dnym = g^r$ where r is known to the ID Authority
- A computes his pseudonym as $p := dnym^x$
- the ID Authority can link p with the user by computing $p^{d^{-1} \bmod q}$ and matching the result with one of the public keys stored in its database

GDPR legal notions

Anonymization

- not defined explicitly in the Regulation but mentioned in the preamble
- like pseudonymization but irreversible
- anonymous identity is to be used where the link to the real ID is need not to be recovered

remark

GDPR says: if the real ID has to be recovered in some situations, then applying anonymization is a violation of GDPR

GDPR legal notions

Example technical realization of anonymization

all computations in a group of a prime order q with hard DHP:

- a user A holds a secret key x, item for domain D there is a corresponding domain public key $dnym = \mathrm{Hash}(D)$
- A computes his pseudonym as $p := dnym^x$

Properties

- nobody knows the discrete logarithm of $dnym$ – thereby a deanonymization is infeasible
- however the user may provide ZKP of equality of discrete logarithms for (g, g^x) and $(dnym, p)$ as well as knowledge of discrete logarithm for g^x

GDPR legal notions

“filing system”

any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

examples

- database
- P2P system
- recommendation system
- cache for search machine
- social networks
- Access Control List for a device
- . . .

GDPR legal notions

actors

controller	... body which determines the purposes and means of the processing of personal data;
processor	... processes personal data on behalf of the controller;
recipient	... a party to which the personal data are disclosed
third party	a recipient that is neither the controller, the processor, nor the data subject

- a controller may be a processor itself
- a controller is a legal position
- a processor is a technical position

GDPR legal notions

“Consent”

any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

- not necessarily in a written form
- it might be just clicking ...
- ... provided that it is not incidental, unconscious
- no consent, if the user is trapped to perform a certain action

GDPR legal notions

“personal data breach”

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;

warning

- destroying personal data might be a “personal data breach”
- any change from the target situation (more access, less access) is a security breach

GDPR legal notions

“binding corporate rules”

personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

- a corporation or a group of corporations may create their own internal policies
- one of standard approaches allowed

GDPR rules of processing

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject
"lawfulness, fairness and transparency";

consequences

transparency: system design must not contain hidden features

transparency: documentation should be available

lawfulness: legal analysis for system design is necessary

GDPR rules of processing

Personal data shall be:

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, ... not be considered to be incompatible with the initial purposes

"purpose limitation";

consequences

- full specification of functionalities
- prevent extensions of functionalities
- matching data and their purpose

GDPR rules of processing

Personal data shall be:

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed "data minimization"

consequences

- less data means lower risk in case of a security breach
- necessary to prevent gathering unnecessary data – tendency to collect too many data
- problems if data cannot be effectively erased

GDPR rules of processing

Personal data shall be:

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
"accuracy"

consequences

- functionalities for data correction
- problems with media that enable only append operation

GDPR rules of processing

Personal data shall be:

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ...
"storage limitation"

possible strategies:

- data erasure
- anonymization
- destroying de-pseudonymization keys if pseudonyms used

GDPR rules of processing

Personal data shall be:

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures
"integrity and confidentiality"

GDPR rules of processing

integrity and confidentiality implementation

signcrypt

a ciphertext contains automatically the signature of the party encrypting the data

authenticated encryption

encryption and MAC generated together:

- replacing a ciphertext by a random string results in an invalid ciphertext
- not true for e.g. AES

GDPR rules of processing

integrity and confidentiality implementation

full disk encryption

- all sectors encrypted
- problems with random access – necessary encryption modes that enable changes per page without enabling to discover identical pages on the disk
- access to disk based on a password
- problem: reduce effectiveness of brute force password guessing – key recovery must be time consuming

GDPR rules of processing

integrity and confidentiality implementation

chaining

- the records create a chain
- record i has a MAC that depends on MAC's of records 1 through $i-1$, e.g.

$$\mathrm{MAC}_i := \mathrm{Hash}(M_i, \mathrm{MAC}_{i-1})$$

- impossible to replace a record i without replacing all records starting from record i
- idea used e.g. in Blockchain

GDPR rules of processing

integrity and confidentiality implementation

Distributed storage

- data record M_i with key k_i stored in locations $\mathrm{Hash}(k_i)$
- additionally duplicate locations: e.g.

$$\mathrm{Hash}(k_i, 1), \ldots, \mathrm{Hash}(k_i, m)$$

- destroying location t deletes only some number of records that have copies elsewhere
- it is very unlikely that two records have all copies at the same locations
- Hash has the nice property that it is
  - deterministic
  - very fast to compute
  - behaves like a random function

GDPR rules of processing

“Accountability”

The controller shall be responsible for, and be able to demonstrate compliance with ...

Consequences

formerly:
- responsibility

now:
- responsibility
- provable security&privacy

demonstration not regarding an abstract model but **reality**

GDPR lawful processing

Conditions for lawful processing

1. the data subject has given consent to the processing ... for one or more specific purposes;
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. processing is necessary for compliance with a legal obligation to which the controller is subject;
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject ...

GDPR - processing for a changed purpose

Conditions for processing with another purpose

ascertain whether processing is compatible with the original purpose
take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offenses are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymization.

GDPR rules for consent

Conditions for consent

1. ... the controller shall be able to demonstrate that the data subject has consented to processing ...
2. The data subject shall have the right to withdraw his or her consent at any time.
3. ... It shall be as easy to withdraw as to give consent.

problems to be solved

- storing and securing consents in an undeniable way
- communication channel for withdrawal
- effective procedures for actions following withdrawal – finding data and erasing
- some kind of authentication of the data subject is necessary

GDPR - challenges concerning children's data

child's consent in relation to information society services

- 1. [if data subject's consent required], in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old.
- Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.
- Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology.

GDPR - challenges concerning children's data

Practical problems

- How to verify the age of a data subject? Declaration? From a child?
- How to verify the parental relation?

Some countries

- electronic personal identity document offers age verification
- answers to queries "is the holder of the ID document older than [legal age] "

GDPR -sensitive data

General restrictions for processing sensitive data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

however, there are some exceptions

consequences

- categorization of data necessary (sensitive and non-sensitive)
- hands off the sensitive data – special very strict policies

GDPR -sensitive data

Exceptions

1. explicit consent of the data subject
2. obligations and specific rights in the field of employment and social security and social protection so far as it is authorized by law
3. protect the vital interests of the data subject if physically or legally incapable of giving consent
4. legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim – processing relates solely to the members ... and not disclosed outside that body;
5. personal data which are manifestly made public by the data subject;

ad 4

Special design for IT systems for churches, trade unions...:

- obliged to provide “appropriate safeguards”
- safeguards must be documented and effective

GDPR -sensitive data

Exceptions

6. exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
7. substantial public interest, on the basis of law – but proportionate to the aim, respect the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights & interests of the data subject;
8. preventive or occupational medicine, working capacity of the employee
9. public interest in the area of public health
10. archiving purposes in the public interest, scientific/historical research or statistical purposes ... but provide for suitable and specific measures to safeguard the fundamental rights & interests of the data subject.

ad 8 and 9

Special design for IT systems for churches, trade unions...:

- obliged to provide “appropriate safeguards”
- safeguards must be documented and effective

GDPR - identification waiver

Processing which does not require identification

- de-pseudonymization may be permanently disabled if the purposes do not or do no longer require the identification of a data subject by the controller,
- “ Where the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible.”

so a communication channel to a pseudonymous data subject might be useful

GDPR - obligations to inform

Information to the data subject

The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

consequences

- necessity of automatic processing and management of information flow
- completeness of information must be controlled
- hard to provide information in *concise, transparent, intelligible and easily accessible form, using clear and plain language*
  - rare skills
  - necessary quality control procedures

GDPR - rules for collecting data

When data collected from the data subject

Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(e) the recipients or categories of recipients of the personal data, if any;

GDPR - rules for collecting data

When data collected from the data subject

(f) the existence of automated decision-making, including profiling, . . . meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

- publicly available rules for e.g. reputation scores for the customers
- customers may adjust and misuse the logic

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

GDPR - rules for collecting data

Additional information

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;

consequence

the controller must have an information channel to the data subject

GDPR - rules for collecting data

If personal data have not been obtained from the data subject

apart from standard informations:

- from which source the personal data originate,

in a timely manner:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

consequences

- data records with data origin information, problems with fixed length records
- automatic management and processing inevitable

GDPR - implementing the rights of the data subject

rights to get information from the controller

- whether their personal data processed by the controller
- if yes, then:
  - purpose
  - categories
  - recipients
  - period (if possible)
  - existence of the right to request from the controller rectification or erasure of personal data or restriction of processing, ...
  - source of data
- for data transferred to a third country or to an international organization: information on the appropriate safeguards

consequences

- having record of all recipients is an obligation
- security documentation for partners outside the common market (EU+)

GDPR -rectification

rights

- The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.
- Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

consequences

- authentication of the data subject
- procedures for completing data
- place for completing data

GDPR - erasure of data on request

Right-to-be-forgotten

The data subject shall have the right to obtain from the controller the erasure of personal data ... without undue delay ... where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes ...

(b) the data subject withdraws consent on which the processing is based according to and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds ...

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services [for children]

GDPR - erasure of data on request

Forgetting published data

Where the controller has made the personal data public and is obliged ... to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

consequences

1. problems for distributed ledgers
2. problems with archives (sequential)
3. problems to find all occurrences
   transitive closure concept does apply??
4. automated (erasure) processing versus examination of legal situation

GDPR - exceptions for requests

When the requests are to be ignored

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health ...

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defense of legal claims.

GDPR - exceptions for requests

When the requests are to be ignored

(a) right of freedom of expression and information;
e.g. requests to remove opinions about cheating in Allegro

(b) legal obligation
e.g. erasing public reviews in case of applying for academic degrees

(c) public health ...
e.g. epidemic data

(d) archiving , scientific, historical research, statistical purposes
data collection by GUS

(e) legal claims.
e.g. unpayed debts database

Challenge

how to categorize properly in a cost efficient way (manual work should be minimized)

GDPR - restriction to processing

Right to restriction of processing

1. The data subject has the right to request restriction of processing, if:
   - (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
   - (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
   - (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims;
   - (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

ad (b) prevent to destroy an evidence

ad (c) the data subject may have interest to keep the data, the controller is obliged to assist

ad (a,b) extra procedures must be started

GDPR - restriction to processing

Right to restriction of processing

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another ... person or for reasons of important public interest of the Union or of a Member State.
3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

consequences

- yet another procedure to implement
- different modes of operation, problems for queries, etc.

GDPR - consequences of erasure or rectification

Obligation to inform

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article ... to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

The controller shall inform the data subject about those recipients if the data subject requests it.

consequences

- necessary to keep track of the recipients:
  - in case they are not anonymous
  - indirectly the regulation creates extra threats for privacy of non-anonymous users
- better not to allow the users to log in...

GDPR - data portability

Right for understandable format

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent ... or on a contract ... and

(b) the processing is carried out by automated means.

transfers between controllers

the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

consequences

- formats like XML
- avoid any format that requires licences to read/modify data

GDPR and marketing

Right to object and automated individual decision-making

- The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions.
- The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

GDPR - limitation of profiling

Automated decisions

1. A data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces significant affects to them.
2. Exceptions:
   (a) entering and performance of a contract;
   (b) is authorized by law
   (c) the data subject's explicit consent.
3. implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
4. decisions shall not be based on sensitive data unless ... [safeguards against discrimination]

GDPR - restrictions of scope

categories where some regulations do not apply

- national security;
- defense;
- public security;
- law enforcement
- other important objectives of general public interest including monetary, budgetary and taxation a matters, public health and social security;
- judicial independence and judicial proceedings;
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- a monitoring, inspection or regulatory function connected to the exercise of official authority in the cases referred above (exception:judicial area)

Responsibility of the controller

General responsibility

- Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons,
  the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

main points

- measures must be proportional
- no ideal security but pragmatic one
- but also no blind trust and processing based on risk
- not only security measures but also a proof of a good conduct

Responsibility of the controller

Policies

- Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
- Adherence to approved codes of conduct or approved certification mechanisms – to demonstrate compliance with the obligations of the controller.

Consequences

- creating and implementing data protection policy is obligatory
- certification mechanisms like CC may be used

GDPR - Data protection by design and by default

technical principles for the controller

1. Taking into account the state of the art, the cost of implementation and the nature, ... the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, ... to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing
2. The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism may be used as an element to demonstrate compliance

GDPR - relations between controller and processor

choice of the processor

- use only processors providing sufficient guarantees for technical and organizational measures appropriate implementation of the Regulation – if the processor has low reputation then the controller violates the regulation
  use some evaluation standards (ISO ...)
- no subcontracting without prior specific or general written authorization of the controller. In the case of general written authorization – inform the controller of any intended changes

GDPR - relations between controller and processor

contract basis

A legal contract or some legal act which sets:

- duration of processing
- nature and purpose of processing
- personal data type
- categories of data subjects
- obligations and rights of the controller

the specification must be complete
no action of the processor without contract authorization

GDPR - relations between controller and processor

contract rules for the processor

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required by law to which the processor is subject;

(b) ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless law requires storage

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations ... allow for and contribute to audits, including inspections, conducted by the controller or another ... mandated ...

GDPR - recording activity

Records of processing activities of the controller

The controller maintains a record of processing activities under its responsibility.
It contains

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients (including in third countries or international organizations);

(e) transfers of personal data to a third country or an international organization, the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organizational security measures

GDPR - recording activity

Records of processing activities of the processor

A written (or electronic) record containing:

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organization, the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organizational security measures

GDPR - security of processing

Technical security obligations

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons,

   the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

   (a) the pseudonymization and encryption of personal data;
   (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
   (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

GDPR - Data protection by design and by default

Technical security obligations

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

GDPR - security breaches

Notification of a personal data breach to the supervisory authority

Controller to the supervisory authority:

- without undue delay and, where feasible, not later than 72 hours after having become aware
- ... unless unlikely to result in a risk to the rights and freedoms of natural persons

Processor to controller:

- without undue delay

Documentation of a breach

responsibility of the controller. the document contains:

- the facts relating to the personal data breach
- its effects
- remedial action taken

GDPR - security breaches

informing the data subject

- not always, only when breach is likely to result in a high risk to the rights and freedoms of natural persons
- in a clear and plain language
- communication not required if:
  - personal data stored in encrypted form
  - risks no longer likely to materialize
  - it would involve disproportionate effort – in this case a public announcement is enough

GDPR -assessment

Data protection impact assessment

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

consequences

- new technology must be carefully examined beforehand
- in particular it must judge upon the necessity and proportionality of the processing operations in relation to the purposes;
- assessment means partially research

GDPR - data protection officer

Obligatory to assign

(a) a public authority or body (exception for courts), or

(b) when processing requires regular and systematic monitoring of data subjects on a large scale, or

(c) processing on a large scale of special categories of sensitive data and data relating to criminal convictions and offenses

... but elsewhere is also a good practice

Qualifications of data protection officer

designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks

consequences

the qualifications, knowledge and ability must be provable

GDPR - role of the data protection officer

Relations between the controller/processor and data protection officer

involvement	officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data
support	support the officer in performing the tasks ... by providing resources ... and access to personal data and processing operations, and to maintain his or her expert knowledge.
independence	the controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.
contacts	a data subjects may contact the officer with regard to all personal data issues
confidentiality	the officer shall be bound by secrecy or confidentiality concerning task performance
other duties	possible, but no conflict of interests should arise

GDPR – codes of conduct

Solutions for SME

- codes of conduct as a standard solution for simple cases
- creation of codes of conduct should be encouraged by the public authorities
- in some countries the solutions are created:
  example: German insurance companies:
  https://www.gdv.de/resource/blob/23938/4aa2847df2940874559e51958a0bb350/download-code-of-conduct-data.pdf

creation of codes of conduct

- Among other contents: mechanisms which enable the mandatory monitoring of compliance with its provisions by the controllers or processors applying it,
- Associations etc. submit the draft code to the supervisory authority.
- The supervisory authority provides an opinion on the draft.
- If draft approved, then the supervisory authority registers and publishes the code.
  (nothing registered yet in Poland)

GDPR - supervision for codes of conduct

a system for auditing compliance

A body may be accredited to monitor compliance with a code of conduct:

independence independence and expertise demonstrated to the supervisory authority;

established procedures for performing assessment and monitoring compliance and to periodically review its operation;

handling complaints established procedures and structures, made transparent to data subjects and the public;

conflict of interests demonstrated to be non-existent

GDPR Certification

Intended certification system

The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors.

reality

1. so far pre-mature concept: certification requires a detailed technical concept – so far not existing
2. no concrete steps by the authorities
3. certification would give a mark valid for 3 years, how to trust certificates about future behavior?

GDPR - transfers to third countries

General rule

transfers allowed only if the rules for transfer from GDPR satisfied – this concerns also further transfers from third countries

approved countries/organizations/sectors

- via a decision of EU Commission:
  a third country, a territory or one or more specified sectors within that third country, or the international organization ensures an adequate level of protection.
- then a transfer shall not require any specific authorization

Current list

The European Commission has so far recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection. Adequacy talks are ongoing with South Korea.

GDPR -transfers subject to appropriate safeguards

if the target country not on the EU list

- a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
- available safeguards:
  - (a) legally binding and enforceable instrument between public bodies
  - (b) binding corporate rules
  - (c) standard data protection clauses adopted by the EU Commission
  - (d) standard data protection clauses adopted by a supervisory authority and approved by the EU Commission
  - (e) an approved code of conduct with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards,
  - (f) an approved certification mechanism ...
- also contractual clauses approved by the supervisory authority

GDPR -binding corporate rules

contents of binding corporate rules

(a) corporate structure, contacts of enterprises engaged

(b) the data transfers and the categories of personal data, the type and purpose of processing, the type of data subjects affected, third countries involved

(c) legally binding nature

(d) the application of the protection principles: purpose limitation, data minimization, ..., and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules

(e) the rights of data subjects in regard to processing and the means to exercise those rights,

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union ...

(g) how the information on the binding corporate rules is provided to the data subjects

(h) the tasks of any data protection officer, monitoring training and

GDPR -supervisory authority

position of supervisory authority

- responsible for monitoring the application of GDPR
- complete independence in performing its tasks and exercising its powers
- a member of each supervisory authority: shall remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

GDPR supervisory authority tasks

(a) monitor implementation and enforce GDPR;

(b) promote public awareness and understanding;

(c) advise the parliament, the government, and other institutions and bodies on personal data protection;

(d) promote the awareness of controllers and processors;

(e) upon request, provide information to any data subject concerning the exercise of their rights

(f) handle complaints

(g) cooperate with other supervisory authorities to ensure the consistency

(h) investigations on the application of GDPR

(i) monitor relevant developments having impact on the protection of personal data

(j) adopt standard contractual clauses

(k) manage a list for data protection impact assessment

(l) give advice on the processing operations

GDPR supervisory authority tasks

(m) encourage the drawing up of codes of conduct

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks

(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct

(q) conduct the accreditation of a body for monitoring codes of conduct

(r) authorize contractual clauses and provisions

(s) approve binding corporate rules

(u) keep internal records of infringements of GDPR

(v) other tasks related to the protection of personal data.

GDPR supervisory authority tasks

How it works in practice

(a) monitor implementation and enforce GDPR; – almost no feedback

(b) promote public awareness and understanding; – minimal

(c) advise the parliament, the government, and other institutions and bodies on personal data protection; – no visible help

(d) promote the awareness of controllers and processors; – some conferences, no guidelines available

(e) upon request, provide information to any data subject concerning the exercise of their rights –???

(f) handle complaints – ???

(g) cooperate with other supervisory authorities to ensure the consistency – no visible coordination

(h) investigations on the application of GDPR – no systematic cooperation with research institutions

(i) monitor relevant developments having impact on the protection of personal data – human capital with technical competence??

(j) adopt standard contractual clauses – no recommendations published

GDPR supervisory authority tasks

how it works in practice

(k) manage a list for data protection impact assessment – no list published

(l) give advice on the processing operations – almost no advice in the crucial implementation phase

(m) encourage the drawing up of codes of conduct – no codes of conduct encountered in PL

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks – so far non-existing in PL, no traces in D

(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct - not published yet

(q) conduct the accreditation of a body for monitoring codes of conduct – yet not happened

(r) authorize contractual clauses and provisions - ???

(s) approve binding corporate rules – unknown

(u) keep internal records of infringements of GDPR – unknown

GDPR - supervision authority

Rights as a controller

(a) request any information from the controller and the processor that it needs (e.g. for evaluation of technological situation)

((b) perform data protection audits

((c) review data protection certifications

((d) notify to controllers/processors of infringements of GDPR

((e) request access to all personal data and to all information – as far as it concerns the supervision

((f) get access to any premises of the controller and the processor (including IT systems)

GDPR -supervising authority

Corrective powers

(a) issue warnings that intended processing operations are likely to infringe provisions of GDPR

(b) issue reprimands

(c) order to comply with the data subject's requests

(d) order the controller or processor to bring processing operations into compliance with GDPR (in a specified manner and within a specified period)

(e) order the controller to communicate a personal data breach to the data subject;

(f) impose a temporary or definitive limitation including a ban on processing

(g) order the rectification or erasure

(h) withdraw a certification (if the requirements are not met)

(i) impose administrative fines (depending on circumstances of each individual case)

(j) suspend data flows to a recipient in a third country

GDPR - international cooperation of supervisory authorities

Consistency mechanism

- rules of cooperation between the supervisory authorities and the EU Commission
- European Data Protection Board – as European supervisory authority – advisory/strategic and not current operations

Role of the Board

- opinions in diverse cases
- dispute resolution, e.g. binding decision which supervisory authority is competent,binding decision if a supervisory authority is not following the opinion of the Board

GDPR - complaints, compensation and liability

The right for complaints

- lodge a complaint with a supervisory authority,
- go to a court to challenge the decision
- go to a court against controller&processor

compensation and liability

- the right for a compensation from the controller or processor for any material or non-material damage as a result of an infringement of GDPR
- the controller liable for the damage caused by processing violating GDPR
- the processor liable only where has not compiled/disobeyed (lawful instructions of) the controller,
- exempt from liability if it proves that it is not in any way responsible

- the processor has to strictly 1) obey the law, 2) obey the controller
- no liability for security breaches resulting from novel, unexpected attacks

GDPR - administrative fines

General rule

Imposed by the supervision authority. In each individual case:

- effective
- proportionate
- dissuasive

practice

- for a long time no fines even in very drastic cases
- before GDPR the fines where not dissuasive for big organizations
- the threat of GDPR has been used to persuade the controllers to pay for extra services
- currently most organizations (including public bodies) have not implemented GDPR or have done it superficially, no reaction from the authorities
- compared to Poland: Germany relatively well advanced even if number of imposed fines very low
- main point for negotiations with big US corporations

GDPR - administrative fines

Factors indicating height of the fine

(a) the nature, gravity and duration of the infringement: ... the number of data subjects affected and the level of damage suffered by them;

(b) intentional or negligent

(c) any action to mitigate the damage

(d) the degree of responsibility taking into account technical and organizational measures implemented

(e) previous infringements

(f) the degree of cooperation with the supervisory authority

(g) the categories of personal data affected

(h) whether, and if so to what extent, the controller or processor notified the infringement

(i) compliance with previously ordered measures

(j) adherence to approved codes of conduct or approved certification mechanisms

(k) other factors: e.g. financial benefits/losses avoided from the infringement

GDPR - administrative fines

The maximal height

it depends on the violation

1. max(10 000 000 EUR, 2% of the total worldwide annual turnover of the preceding financial year)
2. max(20 000 000 EUR, 4% of the total worldwide annual turnover of the preceding financial year) (cases like sensitive data...)
3. non-compliance with an order by the supervisory authority – as in point 2

- for a enterprise the upper bound is 20 000 000 EUR which might be enormous related to its turnover
- since violations are quite common, there is a threat of selective fines
- a good implementation of GDPR eliminates one of the critical business risks, especially for smaller enterprises

International aspects

Third Countries Regulations

Brexit case

possible outcome:

- according to the deal with EU:
  GDPR still applies, after some period new agreement must be achieved
- leaving without deal:
  immediately UK considered as a “third country”, a lot of work to adjust the systems, adjust documentation, decisions, etc.
  risk to spend money on this ...

total chaos!

Third Countries Regulations

Taiwan

- **legislation**: no single act
- **personal data**: information which may be used to identify a natural person, whether directly or indirectly,
- **use versus processing**: use separated from processing,
- **processor**: no data controller
- **transparency**: no hidden processing by unknown parties
- **lawful basis for processing**: explicit rights for processing data are required
- **data minimization and proportionality**: as a security rule
- **retention**: limited
- **right to deletion**: similar to right-to-be-forgotten
- **formalities**: no registration, no supervision authorities

Third Countries Regulations

Taiwan

- **data protection officers**: no obligation to appoint
- **international data transfers**: may be restricted by ministries, e.g. telecommunication in case of transfers to P.R.C.
- **monitoring employees**: court decision: monitoring allowed however only as far as protection of employer's property, safety,...
- **data security and data breach**: responsibility of the data processor to prevent breaches
- **sanctions**: no criminal charges, only civil responsibility

Third Countries Regulations

Canada

- **legislation**: federal Personal Information Protection and Electronic Documents Act (PIPEDA) and some different regulations in different states
- **notions**: no explicit definitions like in EU
- **basic principles**: like in EU: transparency, lawful basis for processing, data minimization and proportionality, data minimization, proportionality
- **accountability**: obligation to define policies, etc. – complete documentation required
- **safeguarding**: specific regulations for different kinds of data
- **accuracy**: obligation to keep correct information
- **right to access**: no obligation to present copies, standard access suffices

Third Countries Regulations

Canada

- **data protection officers**: must be appointed
- **data processors**: formal contracts necessary
- **international data transfers**: possible, but as long as the data are protected abroad
- **monitoring employees**: court decision: monitoring allowed however only as far as protection of employer's property, safety,...
- **data security and data breach**: responsibility of the data processor to prevent breaches
- **sanctions**: no criminal charges, only civil responsibility

Third Countries Regulations

USA

- federal level and state level, major differences between states
- a state may impose restrictions to protect its residents or consumers
- no overall protection, sector rules
  - The Gramm Leach Bliley Act – financial market
  - The Health Information Portability and Accountability Act – health
  - Federal Trade Commission Act – against unfair and deceptive practices
  - Driver& Privacy Protection Act – protection of drivers' personal data
  - Fair Credit Reporting Act -individual credit worthiness, etc
  - CAN-SPAM Act - emails, enables opt-out from unsolicited emails
  - Telephone Consumer Protection Act - privacy of phone calls, text messages
  - Children's Online Privacy Protection Act – children protection
  - Video Privacy Protection Act - CCTV

Third Countries Regulations

USA

- different understanding of “personal data” from state to state, from regulation to regulation
- no “data subject” but either a consumer or a resident of a state
- territorial scope may be understood in the US way: to protect its own people even if regulated by other national law in a third country or state
- focused on security, most European principles (like data minimization, transparency) are not addressed
- rights of the data subject – very limited, e.g. the right to stop processing email address used for advertising, right-to-be-forgotten - only for children and only in California
- data protection officer - obligatory in certain sectors
- The Computer Fraud and Abuse Act: against abusing cookies and similar technologies for behavioral advertising
- international transfers not limited.
- compulsory reporting on security breaches in some sectors

Third Countries Regulations

EU versus USA

very hard to harmonize with EU, however an organization can adopt some rules to comply

Third Countries Regulations

US Privacy Shield

- designed by the U.S. Department of Commerce and the EU uropean Commission and Swiss Administration
- enables automatic decision to transfer data regardless of absence GDPR in target countries
- Privacy Shield is a set of rules for running an organization with regard to dealing with the personal data
- a pragmatic list of principles to be obeyed

Privacy-by-design technical challenges

Realization of technical requirements

available means

- organizational
- technical
- hybrid

trust based solutions

- requirements
- declaration of the manufacturer/system provider for compliance
- trusting the declaration

This is not demonstrable compliance.

Identification challenge

Starting a session between IoT devices

- in most scenarios if two devices interact, then they have to learn who they are
- typically requires sending identifiers
- if (implicit) identifiers are sent over an open channel, then an eavesdropper may learn identities
- tracing enabled – lack of privacy by-design

asymmetric crypto

- protocol:
  1. establish a secure channel - e.g. with Diffie-Hellman
  2. exchange identity data over secure channel
- privacy of identifiers “by design”
- but for IoT devices asymmetric crypto might be too expensive
- but MitM attack must be somehow prevented

Identification challenge

symmetric crypto

- secure channel based usually on a shared key

$$K_{\text{session}} = f(K_{\text{shared}}, \text{nonce})$$

  but the shared key identified after exchanging identifiers in plaintext
- so global tracing becomes possible
- shared key discovery, a simple protocol:
  - A sends (h, nonce) where $h := \text{Hash}(K, \text{nonce})$
  - B receives (h, nonce) and looks for κ in its database for which

$$h = \text{Hash}(\kappa, \text{nonce})$$

- problem: time complexity, no scalability – for small systems only

Key predistribution

the second approach

Predistribution

1. there is a pool of keys of size N
2. each device gets a subsets of n keys
3. the subsets are chosen so that two random devices have a shared key or keys

Establishing connection

1. find out which key or keys are shared,
2. use these keys to negotiate a session key

Key predistribution

the second approach

Establishing connection-example

1. Alice sends a random nonce r_a to Bob
2. Bob chooses random nonce r_b, and sends

$$\mathrm{Enc}_K(r_a, r_b)$$

   to Alice (K is the shared key)
3. Alice decrypts, and rejects if the first part is not r_a
4. Alice computes

$$\mathrm{Enc}_K(r_b, r_a)$$

   and sends it to Bob
5. Bob decrypts and checks the plaintext

Problem

everything fine, but how to find shared keys?

- indicate choice of keys – but this is an implicit ID!
- try each combination of keys one by one – inefficient

ad hoc idea

particular predistribution method:

- divide the pool into n disjoint *key bags*
- a device gets just one key per key bag

Special Predistribution

Establishing connection

- for each bag a separate investigation
- for a bag: the algorithm from the previous slides

communication complexity for k bags: $2k + 1$ messages

Special Predistribution

Establishing connection

variation

for the case when we expect to have 2 shared keys

- Alice chooses a nonce for each bag, the nonces are different but in some sense related
- for each i, Alice encrypts nonce for bag i with the key from bag i
- Bob gets the ciphertexts, decrypts them and recognizes the shared keys via relation between the corresponding plaintexts

communication complexity for k bags: k messages

Advantage of 2 shared keys

Following Alice and Bob: 1 shared key case

- if the adversary knows the single key k shared by Alice and Bob, then it can identify all suspects to be Alice and Bob and decrypt their messages
- there are many other devices knowing k

Following Alice and Bob: 2 shared keys case

- when k_1 and k_2 shared:
- necessary to know both k_1 and k_2 to spy
- more possibilities, much less likely

A nice feature

If only one key shared then it is not revealed which one is shared and insecure connection based on this single key is avoided.

“private predistribution”

main points

1. the general key predistribution scheme used only for establishing the first connection between Alice and Bob (initialization)
2. after that each party holds:
   - keys used to authenticate against its partners (internal keys)
   - keys of the partners (external keys)

we assume that the number of devices is very big however the number of partners for each device is quite limited (like in the human society)

A detailed solution

assumptions

- each two users share a unique secret key established by them during the initialization,
- the set of internal and external keys are the same

Algorithm

1. Bob chooses n_0 at random and sends it (to Alice)
2. Alice creates
$$c_1 := \mathrm{Enc}_{k_1}(n_0, nonce_1), \ldots, c_m := \mathrm{Enc}_{k_m}(n_0, nonce_m),$$
(Alice does not know with whom it is talking, nonces are random)
3. Alice sends $c_1, \ldots, c_m$ (to Bob)
4. Bob decrypts, for the shared key k_j the result yields $n_0, nonce$
5. Bob responds with $c := \mathrm{Enc}_{k_j}(n_1)$ where $n_1 := (truncHash(n_0), nonce)$
6. Alice decrypts c with all keys from its pool and tests the resulting n_1 if it starts with $truncHash(n_0)$, only for shared k_j the result is correct

Scheme 1: complexity

properties

1. a user holds n keys where n is the set of partners
2. communication volume: $n + 1$ ciphertexts
3. number of decryption/encryptions: $n + 1$
4. each partner of Alice will be recognized by Alice
5. in order to continue Alice derives a session key based on nonces and the shared key (implicit choice),

Evolution of identifiers -defense against tracing

Evolving identification

1. for the connection between Alice a and Bob b there are two identifiers i_{ab} and i_{ba}
2. i_{ab} is used as identifier from Alice to Bob, and is kept by Alice
3. similarly with i_{ba}
4. the identifiers change at each interaction e.g. $i_{ab} := \mathrm{Hash}(i_{ab}, i)$ where i is a small number
5. backward security: from the current i_{ab} it is impossible to derive its previous and find all interactions
6. the parameters i enable to loose track, if the adversary knows i_{ab} but then is unable to monitor interaction during some time period

Example shared key discovery

Algorithm

1. Bob chooses random n_b and n'_b such that $R(n_b, n'_b)$
2. for each key k_i from the external pool, Bob computes $c_i := \mathrm{Enc}_k(n_b)$ and $c'_i := \mathrm{Enc}_k(n'_b)$
3. Bob sends the resulting ciphertexts $c_1, c'_1, \ldots, c_m, c'_m$ to Alice
4. for $i \leq m$, Alice decrypts c_i, c'_i with each of the keys from its internal pool, if two plaintexts are in relation R, then the key and the result of decryption are accepted
5. finally Alice checks that the decrypted and accepted nonces are the same for two accepted keys (additional error prevention)
6. in the opposite direction a nonce n_a is encrypted and sent, where e.g.

$$n_a = r||\text{truncated-hash}(n_b)$$

Example shared key discovery

Algorithm

in the opposite direction:

option 1: pairwise shared keys are used
then

- Bob has to make $\leq m$ decryptions
- communication volume: 1 ciphertext

option 2: the same mechanism as in the first part of the algorithm:
then

- Bob has to make $\leq 2m$ decryptions
- communication volume: $2m$ ciphertexts

complexity of the first part

(Bob does not know who of its friends is in the range)

- Bob make $2m$ encryptions
- Alice makes $< 2m\sqrt{n}$ decryptions
- communication volume: $\sqrt{n}$ ciphertexts

Privacy issues

What can be observed?

1. Eve, a partner of Alice may participate in communication and learn that Alice is there

   inevitable if there is no prior knowledge

2. even if Bob and Eve share some key, Eve cannot detect that this key has been used

   the plaintext is random, and the keys used in the second ciphertext of a pair are different for Bob and Eve

Deniability challenge

Selling authentication proofs to third parties

- prover A authenticates to verifier B:
  - B chooses a challenge r at random
  - A creates a signature $s := \mathrm{Sign}_K(r)$
  - B verifies s
- Problem: B can show s to a third party as a proof of interaction with A

How to adjust the design so that it is impossible?

Protocol example - Stinson-Wu scheme

Keys

Prover holds a private key a corresponding to the public key $A = g^a$

Authentication of the Prover

1. Verifier: chooses $x \leftarrow_{\$} \mathbb{Z}_q^*$, computes $X = g^x$, $Y = \mathrm{Hash}(A^x)$ and sends X, Y to the Prover
2. Prover computes $Z = X^a$ and aborts if $Y \neq \mathrm{Hash}(Z)$, otherwise it sends Z to the Verifier
3. Verifier accepts iff $Z == A^x$.

why the proof is not transferable?

A transcript of interaction cannot serve as a proof of interaction:

> *Verifier can himself create the answer of the Prover, therefore the Verifier may cheat*

Cleverness of protocol design from the point of view of GDPR

typical attack

- Ask the verifier to take X such that its discrete logarithm is unknown.
- Then the prover serves as an oracle for computing a value that would be unable to create by anybody else.
- Thereby a strong (and dangerous) data created as a side-effect of identification.

situation for Stinson-Wu protocol

There is no such danger via a clever design:

- the verifier may send arbitrary (X, Y)
- ... however the verifier aborts if $Y \neq \mathrm{Hash}(X^a)$
- the only way to provide valid (X, Y) by the verifier is to know x such that $X = g^x$
- ... but then the verifier can create the answer himself and the presence of the prover is unnecessary

Trusting software/hardware manufacturers

Dilemma of personal data controller

1. how to check that the product provider has not installed trapdoors or weak points?
2. the situation especially hard for random number generators
3. a physical generator is uncontrollable (apart from heavy faults)
4. therefore there are NIST recommendations to use Pseudorandom Number Generators (PRNG)
5. ... but a PRNG provides no security if the seed is compromised
6. at the very end the controller would be in a big trouble in case of such a situation
7. certification may not suffice! A certificate cannot prove that the seed is not retained by the manufacturer.

Problem

1. is authentication possible with symmetric algorithms without randomness?
2. If there is randomness, how do we know for instance that it does not contain fingerprints for the eavesdropper?
3. hidden channel might be impossible to detect in a regular way: e.g. $r := \mathrm{Hash}(k, i)$ where k is shared and i is the message from a small range

Verifiability model

1. a user himself can locally check that the system is not cheating and not installing trapdoors
2. research on such schemes originates from e-voting

Watchdog model

architecture

1. a third device between Alice and Bob
2. a watchdog for Alice

In practice, the device named Alice has a device form a different source attached, called Watchdog.

Enhanced challenge-response

challenge-response

1. Alice chooses r and sends to Bob
2. Bob computes $\mathrm{Enc}(r, nonce)$ and returns the result

r might be malicious

challenge-response 2

1. Alice chooses u and sends $\mathrm{Commitment}(u)$ to the watchdog,
2. the watchdog chooses s at random and returns to Alice,
3. Alice sends the challenge $r = u \oplus s$ as the challenge
4. the watchdog forwards the message iff the hash obtained before is $\mathrm{Commitment}(r \oplus s)$
5. Bob computes $\mathrm{Enc}(r, nonce)$ and returns the result

Problem

authentication algorithm discussed above

- the challenges should not be presented in clear, only ciphertexts are allowed
- however, if $\mathrm{Enc}_K(r_a)$ is sent by Alice, then the watchdog can forward

$$s \oplus \mathrm{Enc}_K(r_a)$$

for a randomly chosen s

- $\Rightarrow$ the plaintext changes in some crazy way to r'_a, but Alice can recover it
- Bob cannot respond with

$$\mathrm{Enc}_K(r_b, r'_a)$$

if the watchdog is used on his side.
slight changes in the protocol needed:

random nonces sent always separately