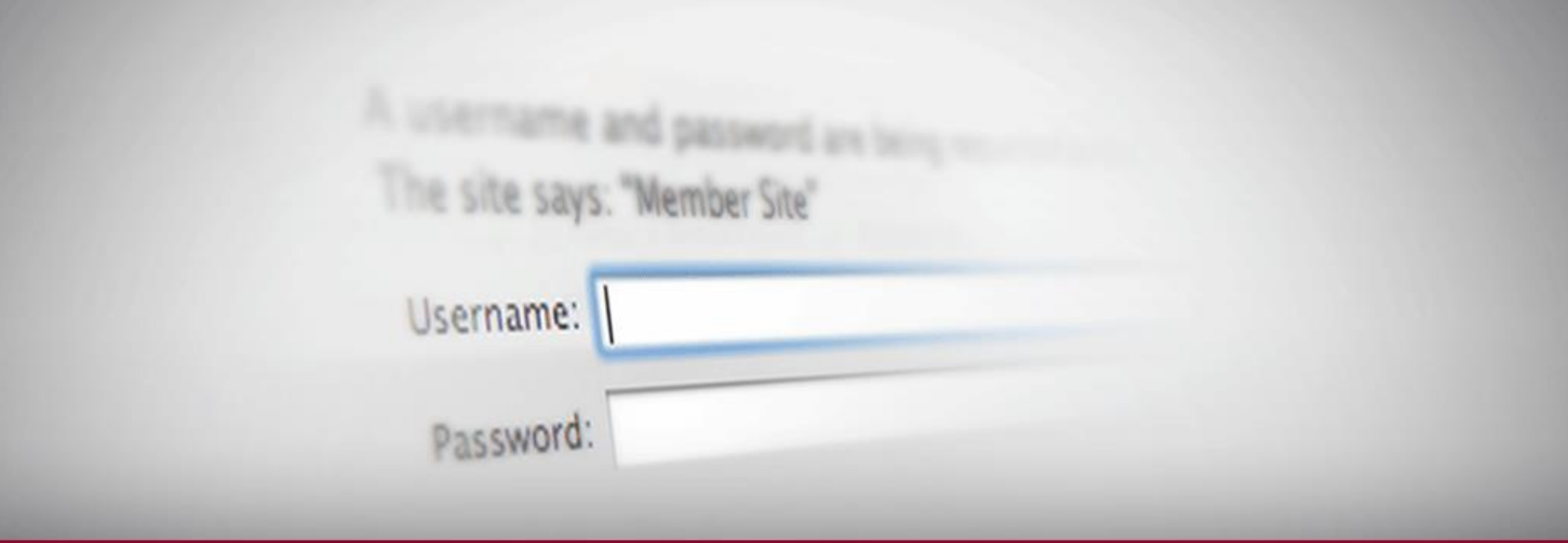


National Authority for Data Protection
and Freedom of Information

European Data Protection Law

Budapest

2017/18, PPKE-JÁK

National Authority for Data Protection
and Freedom of Information

Privacy

- Physical sphere
- Psychological sphere
- Virtual sphere

Old technology


ASAHI
PENTAX
Asahi Opt. Co.
Lens made in Japan
Super-Takumar 1:1.4/50 3594536

Warren and Brandeis

- Right to life – right to quality of life
- Object of the protection – the data itself
- Expectation of privacy (public role)
- Right to be let alone

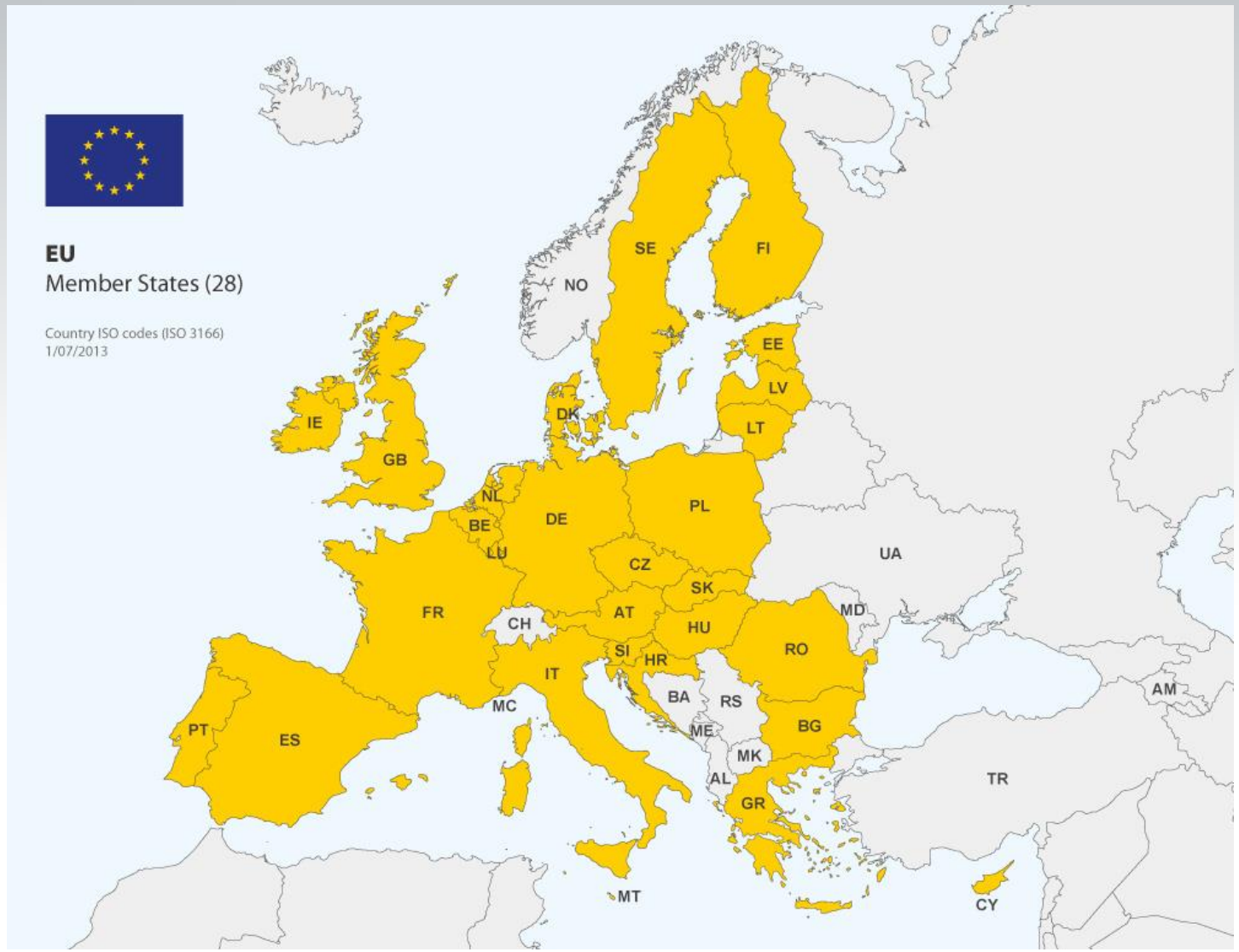
National Authority for Data Protection
and Freedom of Information

New technology

European Union Law

National Authority for Data Protection
and Freedom of Information

EU Member States



Legal background

Primary law

- Treaty on the European Union
- Treaty on the functioning of the EU
- Charter of Fundamental Rights

Secondary law

- Regulation
- Directive
- Decision

National Authority for Data Protection and Freedom of Information

Data protection legal background - old

- Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Council framework decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters
- Data protection reform package
  - General Data Protection Regulation
  - Directive

National Authority for Data Protection and Freedom of Information

Data protection legal background - new

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Definition

- personal data: shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
- special categories of data: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
- processing of personal data: shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

National Authority for Data Protection
and Freedom of Information

Identified or identifiable

National Authority for Data Protection
and Freedom of Information

Good examples

National Authority for Data Protection
and Freedom of Information

Definition

• controller: shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by law, the controller or the specific criteria for his nomination may be designated by law;

• processor: shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

• scope: shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

• exemption: by a natural person for purely personal or household activity (outside of the scope of EU law)

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 analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

Genetic data

Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question

National Authority for Data Protection
and Freedom of Information

Biometric data

Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data

Territorial scope

This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

- the monitoring of their behaviour as far as their behaviour takes place within the Union

Principles

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes – purpose limitation principle;
- adequate, relevant and not excessive;
- data minimisation;
- accuracy:
  - up to dateness;
  - accurate;
  - completeness;
- data security
- privacy by design and by default
- accountability

National Authority for Data Protection
and Freedom of Information

Purpose limitation principle

- collected for specified, explicit and legitimate purposes;
- adequate, relevant and not excessive;
- essential for the purpose;
- duration necessary to achieve its purpose.

National Authority for Data Protection
and Freedom of Information

Legal basis

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) 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;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) 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;

(f) 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 which require protection of personal data, in particular where the data subject is a child.

Consent

- WP 29 opinion 15/2011
  - – unambiguous" consent - only consent that is based on statements or actions to signify agreement constitutes valid consent;
  - – requiring data controllers to put in place mechanisms to demonstrate consent;
  - – the quality and accessibility of the information forming the basis for consent.

- Criteria: information to be given to the data subjects in advance

Balance of interest

Article 7 (f) of the directive 95/46

(f) processing is necessary for the purposes of the **legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject** which require protection under Article 1 (1).

Data subject's rights

- information to be provided to the data subject (without request)
- right of acces (on request)
- right to rectification
- right to erasure (right to be forgotten)
- right to restriction of processing
- right to data portability
- right to object

Data portability

Consent or contract
Concerning the data subject and provided by them

E-mail box
Contact list
Group chats
Blog posts and comments
Information provided for an insurance policy
Banking transactions

Right to object

Processing based on point (e) or (f) or Article 6
Profiling
Direct marketing purposes

Opt out
Opt in

Right to erasure and to be forgotten

Erasure

No longer necessary or unlawful

Withdraws consent or objection (lack of overriding legitimate interests)

Legal provision requires erasure

Child – information society service

To be forgotten

The controller has made the personal data public

Inform controllers about the request – links, copy, replication of the data concerned

"OK I've abused women, molested girls –
but I've exerted my right to have my past forgotten."

Right to erasure and to be forgotten

Exceptions

Freedom of expression
Compliance with legal obligation
Public interest – public health
Archiving in public interest
Legal claims (establishment, exercise, defense)

Remedies

- data controller
- supervisory authority
- judicial remedy

National Authority for Data Protection and Freedom of Information

Article 28 (1) of the Directive

- Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.
- These authorities shall act with complete independence in exercising the functions entrusted to them.

Article 29 Working Party

- advisory status;
- act independently;
- composed of:
  - a representative of the supervisory authority or authorities designated by each Member State
  - a representative of the authority or authorities established for the Community institutions and bodies,
  - a representative of the Commission,
- take decisions by a simple majority;
- elect its chairman for two years.


CNIL


H

National Authority for Data Protection
and Freedom of Information

Independence of DPAs

- Personal
- Organizational
- Financial
- Operational

National Authority for Data Protection and Freedom of Information

Independence of DPAs - Germany

Commission v. Germany (c-518/07, Judgment of 9 March 2010)

- The Commission requested the Court to declare that, since the laws in different Länders expressly subjected the DPAs to State supervision, Germany has failed to fulfill its obligations under Article 28 (1) of the Directive
- Article 28 (1) is to be interpreted as meaning that DPAs must enjoy independence allowing them to perform their duties **free from external influence**
- State scrutiny allows the government of the respective Land to **influence**, directly or indirectly, the decisions of DPAs or to **cancel** and **replace** those decisions
- **Mere risk** of political influence is enough to hinder independence of the DPAs
- Germany failed to fulfill its obligations under Article 28 (1) of the Directive
- From 1 January 2016 the law has been amended accordingly

National Authority for Data Protection and Freedom of Information

Independence of DPAs – Austria

Commission v. Austria (C-614/10, Judgment of 16 October 2012)

- The Commission requested the ECJ to declare that Austria has failed to fulfill its obligations under Article 28(1) of the Directive
- The fact that the office of the Datenschutzkommission (DSK) is composed of officials of the Chancellery carries a **risk of influence** over the DSK
- The managing member of the DSK is a **federal official** subject to supervision, which cannot exclude that his or her superior might exercise indirect influence
- Austria has failed to fulfill its obligations under Article 28(1)
- New authority was set up

National Authority for Data Protection and Freedom of Information

Independence of DPAs – Hungary

Commission v. Hungary (Judgment 2014)

- The Commission requested the ECJ to declare that the early termination of the Commissioner was in breach of Art. 28 (1)
- The Court found that the request of the EC was justified
- The Govt. and previous Commissioner agreed on a compensation
- The EC closed the infringement procedure

Data retention

- aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communication networks with respect to the retention of certain data;
- the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law;
- periods of retention: not less than six months and not more than two years
- CoEU ruled that the directive is invalid

National Authority for Data Protection
and Freedom of Information

Hungarian DPA

National Authority for Data Protection
and Freedom of Information

Hungarian DPA

- established in 1995
- adequate level of protection acknowledged in 2000
- ombudsman system transformed
- a real authority from 2012

National Authority for Data Protection
and Freedom of Information

Dual set of tools

in an ombudsman-type role

- investigate
- legislative opinions
- participation in court proceedings
- annual report
- recommendations
- aspects of audit
- international representation
- conference of data protection officers

as an authority

- data protection administrativ proceedings
- classified data authority proceedings
- data protection register
- administrative sanctions

National Authority for Data Protection and Freedom of Information

Data protection administrative procedure

1.

- (notification) >> (examination) >> (action)
  >>initiation of procedure **ex officio**
- procedure required if it is likely that the unlawful data processing has occurred in a way that:

1. affects a wide scope of persons
2. significantly harms interests or carries the risk of damages

2.

- general rules of administrative procedures apply
- administrative deadline: two months
- remedy: judicial review

National Authority for Data Protection
and Freedom of Information

Administrative fines

- Effective, proportionate and dissuasive
- Nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them
- The intentional or negligent character of the infringement
- Any action taken by the controller or processor to mitigate the damage suffered by data subjects
- The degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

National Authority for Data Protection
and Freedom of Information

Administrative fines

- Any relevant previous infringements by the controller or processor
- The degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement
- The categories of personal data affected by the infringement
- The manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement
- Where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures

National Authority for Data Protection
and Freedom of Information

Administrative fines

- Adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42
- Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

- Up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher
- Up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher

Judicial control over administrative decisions

National Authority for Data Protection and Freedom of Information

Significant administrative proceedings

Cases where the Authority imposed a fine and its resolution has been challenged before the court:

1. Fluffy cake
2. The publicity of the insulted party's name in the criminal news
3. Storage of documents in inadequate place
4. Publication of debtors' list on the webpage of a local government
5. Denying access to the report of a medical expert

Fluffy cake

Relevant facts of the case

- Any person could register on the dating site, many registrant was under the age of 16
- The age limit of the informational self-determination is 16 in Hungary
- In the case of the minors under the age of 16 the permission or subsequent approval of their legal representative is requested by law
- In this case, however, these permissons were missing

Fluffy cake

Resolution

- The Authority eximaned 22 websites, in 9 cases the Authority adopted a resolution

  – erasure of the unlawfully processed personal data

  – imposed a fine

National Authority for Data Protection and Freedom of Information

Fluffy cake – challenge of the DPA's decision

Claim

- There is no regulation prohibiting the registration of the minors
- The site is similar to other socail media sites like Facebook
- Those who have the technical abilities to register, have presumably knowledge about the nature or the content of the site
- The real age of the participants cannot be verified - it may occur that an older person registers as minor and in the other way, a minor declares to be over 16

Fluffy cake

Court decision

- In the case of a minor under age of 16 the permisson of their legal representative is necessary for a lawful data processing

- There are methods which can garantee that the parental permission is given

National Authority for Data Protection and Freedom of Information

The publicity of the insulted party's name

Relevant facts of the case

- A daughter of a well-known politician has been victim of a sexual abuse
- The victim's father has itself reported on the attack in his website without giving the name of his affected daughter, only stating her age
- From the father's online CV, where he gave the name and the date of birth of his children, the person of the victim could be easily identified
- On the basis of these publicly available information the media made the full name of the victim public in the news

National Authority for Data Protection and Freedom of Information

The publicity of the insulted party's name

Resolution

- prohibited the unlawful data processing
- imposed a fine of 200 000 Ft

National Authority for Data Protection
and Freedom of Information

The publicity of the insulted party's name

Claim

- The editors argued that they did not infringe any personal right, they just collected public informations from the web

- From the father's report and from his public CV full name of the victim was easily accessible

National Authority for Data Protection and Freedom of Information

The publicity of the insulted party's name

Court decision

- Not the publication of the name is unlawful in itself, but the fact that the name has been linked to the crime
- It is such an important circumstance that for the publication the consent of the data subject would be necessary
- There was no special reason to publish the full name
- It is an infringement of the private sphere and the carrier prospects of the victim can be harmed by this unlawful act of publication

National Authority for Data Protection and Freedom of Information

Storage of documents in inadequate place

Relevant facts of the case

- The company stored the documents of other liquidated companies
- These documents contained different personal data and have been stored in an abandoned, windowless building (stall) without any surveillance
- The personal data have concerned employment, medical, and state insurance records

National Authority for Data Protection and Freedom of Information

Storage of documents in inadequate place

Resolution

- The selection of the documents according to their data content and
- The transmission to the competent authority (state archives, pension insurance fund etc.) or
- Phisycal distruction of the document containing data
- 5 Million Ft (~ 17.000 €) fine

National Authority for Data Protection and Freedom of Information

Storage of documents in inadequate place

The legal background of the decision:

„*Data must be protected by means of suitable measures against unauthorized access, alteration, transmission, public disclosure, deletion or destruction, as well as damage and accidental loss, and to ensure that stored data cannot be corrupted and rendered inaccessible due to any changes in or modification of the applied technique.”*

[Privacy Act s. 7]

National Authority for Data Protection and Freedom of Information

Storage of documents in inadequate place

Claim

- The relevant facts were not fully revealed by the Authority during the investigation
- The gravity of the infringement was not defined properly
- The authority did not take into account that the data controller was under liquidation
- The resolution did not exactly repeat the text of the relevant act

National Authority for Data Protection and Freedom of Information

Storage of documents in inadequate place

Court decision

- The fact that the company was under liquidation does not block the administrative proceeding
- The fact that the number of data subjects were not exactly defined does not make the Authority's resolution unlawful because the large number of affected data subjects was obvious
- The free citation of the relevant legal norm does not mean that the Authority transgressed its competencies

National Authority for Data Protection
and Freedom of Information

Data theft incident

Relevant facts

- A multinational company collected personal data during a promotion campaign. A hacker group stole these data by breaking up the website and made them publish in the internet,
- The affected personal data: name, email address, phone number, date and place of birth,
- To examine whether the data controller has given everything to meet the data security requirements.

Data theft incident

Decision

- concluded that the data controller is responsible for the breach due to the lack of security measures

- imposed 1,5 million Ft fine

Debtors'list

Relevant facts of the case

- The local governement processed additional data besides that was legally prescribed on a debtors' list
- The list also contained the data of a certain environmental fee
- The up-to-dateness of the data has not been provided

Debtors'list

Resolution

- 200.000 Ft (~ 700 €) fine
- The unlawful processing of personal data has been terminated before the resolution, that's why the authority did not impose any other sanction

Debtors'list

The legal backgrounds of the decision

• *Personal data may be processed only for specified and explicit purposes, where it is necessary for the implementation of certain rights or obligations.*

[Privacy Act s. 4]

• *Personal data may be processed under the following circumstances:*

a) when the data subject has given his consent, or

b) when processing is necessary as decreed by law…

[Privacy Act s. 5]

Debtors’list

Claim

- The principle of progressive sanctions was violated
- The relevant facts were not fully revealed by the Authority (e.g. the financial capacity of the data controller)
- The relevant legal norms were not given exactly in the resolution

Debtors'list

Court decision

- The act regulating the general administrative proceedings is only supplementary to the Privacy Act (it works only if there is no special rule in the Privacy Act)
- The Privacy Act regulates how to impose a fine
- The financial capacity of the affected local government is irrelevant in defining the magnitude of a fine
- The burden of proof lies with the local government to prove that the Authority violated the procedural rules

National Authority for Data Protection and Freedom of Information

Access to reports of a medical expert

The data subject has been severely injured in a traffic accident

- The opinion of the medical expert was not provided to him
- The data in question were special medical data

The reasons of denial were:

- That the expert opinion has been regarded as an internal document
- It was argued, that the opinion contained such data which were not related to the data subject
- The report was drawn up for a fee (not for free)

National Authority for Data Protection and Freedom of Information

Access to reports of a medical expert

Resolution

- 500.000 Ft (~ 1700 €) fine
- The relevant medical documents should be provided to the data subject
- The irrelevant data should be anonimysed in the documents before providing them to the data subject

National Authority for Data Protection and Freedom of Information

Access to reports of a medical expert

The legal background of the decision

„Upon the data subject's request the data controller shall provide information concerning the data relating to him, including ... the purpose, grounds and duration of processing, the name and address of the data processor […].”

„Data processors must comply with requests for information without any delay, and provide the information requested in an intelligible form, in writing at the data subject's request, within not more than thirty days.”

[Privacy Act s. 15]

National Authority for Data Protection and Freedom of Information

Access to reports of a medical expert

Claim

- The documents in question have been already provided to the data subject during the investigation
- The expert opinion contained such data which were not personal, and therefore there was no obligation to provide them
- The data controller informed the affected party about the documents
- The Privacy Act does not explicitly prescribe that the data controller should provide the data subject with the whole documentation

National Authority for Data Protection and Freedom of Information

Access to reports of a medical expert

Court decision

- The claim that the data subject should only be informed about the pure fact of the data processing and not about the content of the data is not compatible neither with the aims of the Privacy Act nor with the rights of the data subject
- The Authority has kept the procedural rules
- The penalty has been grounded properly and has been conducted lawfully

Conclusions drawn from the case law

Conclusions

- no transgression of competence, if the decision does not repeat exactly the language of the Privacy Act;
- the act regulating the general administrative proceedings works only if no special rule in the Privacy Act;
- a fine can be imposed even if the unlawful processing of personal data had been terminated before the Authority passed its resolution;
- the resolution is well-founded, if the Authority followed the procedural rules, if the justification of the decision is clear, if the imposement of the fine was necessary and there was a casual connection between the harm and the unlawful activity;
- a reasonable transgression of the administrative time limit does not affect the unlawfulness of the resolution;
- the ability to pay is not relevant when imposing a fine.

Search engines

The European Court of Justice
Data controller

- Google case (C-131/12): The activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as ‘processing of personal data;

- Lindqvist case(C-101/01): personal data publishing on the internet is data processing;

- Satakunnan Markkinapörssi case (C-73/07): already published data are concerned with the activity, can be regarded as data processing;

- WP 169: considered as data controller who specifies the purpose and the mean of the data processing → search engines play a specific roll in global dissemination of data, systematize and classify personal data to make them easily available.

The European Court of Justice Jurisdiction

- Processing of personal data is carried out **in the context of the activities** of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a **branch or subsidiary** which is intended **to promote and sell advertising space** offered by that engine and which **orientates its activity towards the inhabitants of that Member State**;

National Authority for Data Protection and Freedom of Information

The European Court of Justice
Right of erasure

• The operator of a search engine is obliged to **remove** from the list of results displayed following a **search made on the basis of a person's name** links to web pages, published by third parties and containing information relating to that person, also in a case **where that name or information is not erased beforehand** or simultaneously from those web pages, **and even**, as the case may be, when its **publication** in itself on those pages **is lawful**.

The European Court of Justice
Interest consideration

- Data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those **rights override**, as a rule, not only **the economic interest of the operator** of the search engine but also **the interest of the general public in having access to that information** upon a search relating to the data subject's name.
- However, that **would not be the case** if it appeared, for particular reasons, such as the **role** played by the data subject **in public life**, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.

WP29 Guidelines

1. Search engine qualify as data controllers, and must be distinguished from publishers of third-party websites;

2. A fair balance between fundamental rights and interests;

3. DPAs will systematically take into account the interest of the public in having access to the information. If the interest of the public overrides the rights of the data subject, de-listing will not be appropriate;

WP29 Guidelines

4. Only affects the results obtained from searches made on the basis of a person's name and does not require deletion of the link from the indexes of the search engine altogether;

5. Individuals are not obliged to contact the original website in order to exercise their rights towards the search engines;

6. DPAs will focus on claims where there is a clear link between the data subject and the EU;

WP29 Guidelines

7. Territorial effect: guarantee the effective and complete protection of data subjects' rights including .com domains;

8. No requirements to inform the users of search engines that the list of results to their queries is not complete;

9. Search engines should not as a general practice inform the webmasters of the pages affected by removals.

Weltimmo case
Applicable law

National Authority for Data Protection and Freedom of Information

Weltimmo case

Relevant facts

- Data controller operated a property advertisement website;
- Free period: 30 days – after that a fee should be paid for minimum 6 months;
- The advertisement would not be deleted unless the data subject paid the fee;
- Data controller registered in Slovakia, but the other relevant facts connected to Hungary.

Weltimmo case

Jurisdiction

Directive (19): *„establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements.”*

Applicable law

Directive Article 4.: *„Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State.”*

National Authority for Data Protection and Freedom of Information

Transer of personal data to third countries

- Legal basis,
- Adequate level of protection:
  - Decision of the European Commission (Safe Harbor, Privacy Shield),
  - Appropriate safeguards, including standard contractual clauses, binding corporate rules (BCR), codes of conduct, certification mechanism, legally binding legal instruments between public authorities.

Novelties in GDPR

National Authority for Data Protection
and Freedom of Information

Risk-based approach

What is risk?

physical, material or non-material damage

identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage

where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data

National Authority for Data Protection
and Freedom of Information

Risk-based approach

What is risk?

where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures

Risk-based approach

What is risk?

where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles

where personal data of vulnerable natural persons, in particular of children, are processed

involves a large amount of personal data and affects a large number of data subjects

National Authority for Data Protection
and Freedom of Information

Risk-based approach

How to measure risk?

likelihood and severity
should be determined by reference to the nature, scope, context and purposes of the processing.

Risk should be evaluated on the basis of an objective assessment, to establish
whether data processing operations involve a risk or a high risk

National Authority for Data Protection
and Freedom of Information

Data breach notification

Personal data breach

means 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

Data breach notification

Level 1

The breach is unlikely to result in a risk

The controller shall document these breaches and make it available for the supervisory authority

No notification to the SA is required

National Authority for Data Protection
and Freedom of Information

Data breach notification

Level 2

The breach is likely to result in a risk

Notification to the SA is required in 72 hours

Notification includes:
Nature of the breach
Categories of data subjects and personal data records
Likely consequences
Measures taken

National Authority for Data Protection
and Freedom of Information

Data breach notification

Level 3

The breach is likely to result in a high risk

Notification to the SA is required in 72 hours

Notification of the data subjects or the public

Notification includes:
Nature of the breach in clear and plain language

National Authority for Data Protection
and Freedom of Information

Privacy impact assessment

Use of new technologies

Processing is likely to result in a high risk

Prior to the processing

National Authority for Data Protection
and Freedom of Information

Privacy impact assessment

Shall be carried out in case of

Systematic and extensive evaluation of personal aspects based on automated processing, including profiling, on which decisions are based that produce legal effects

Processing on a large scale of special categories of data

Systematic monitoring of a publicly accessible area on a large scale

National Authority for Data Protection
and Freedom of Information

Privacy impact assessment

Content of the assessment

Description of the processing

Necessity and proportionality

Assessment of the risks

The measure to be implemented to address the risks

Privacy impact assessment

Where the assessment indicates high risk, the SA shall be consulted

Written advice

Powers of the SA may be exercised

National Authority for Data Protection and Freedom of Information

Data protection officer (DPO)

Appointed by the controller or processor in specific cases

Public authority or body

Core activity consists of processing that requires regular and systematic monitoring of data subjects on a large scale

Core activities – processing special categories on a large scale

National Authority for Data Protection
and Freedom of Information

Data protection officer (DPO)

Involved in all issues related to DP

Carries out the tasks in an independent manner (does not receive any instructions regarding the exercise of the duties)

Inform and advise the controller
Monitor compliance with the Regulation
Cooperate with the Supervisory Authority

National Authority for Data Protection
and Freedom of Information

Procedures under the GDPR

One-stop-shop mechanism

Mutual assistance

Joint operations

Urgency procedure

EDPB – issuing binding opinion

EDPB – dispute resolution, binding decision

National Authority for Data Protection
and Freedom of Information

One-stop-shop

Cross-border processing

Establishments in more than one member state

Processing taking place by a single establishment which substantially affects data subjects in more than one member state

National Authority for Data Protection
and Freedom of Information

One-stop-shop

Lead authority

Concerned authority

In an endeavor to reach consensus

Draft decision

Relevant and reasoned objection

Dispute resolution within the EDPB

National Authority for Data Protection
and Freedom of Information

Mutual assistance

Not necessarily cross-border processing

Information requests

Supervisory measures

Inspections

Investigations

One month deadline

National Authority for Data Protection
and Freedom of Information

Joint operations

Joint investigations

Joint enforcement measures

Staff of several SAs are involved

National Authority for Data Protection
and Freedom of Information

Opinion of the EDPB

SAs shall seek the opinion of the Board

Data protection impact assessment

Draft code of conduct

Criteria for accreditation

Approval of criteria related to transfer of personal data to third countries

National Authority for Data Protection
and Freedom of Information

Dispute resolution

No agreement during the one-stop-shop mechanism

No agreement on which SA is competent for the establishment

The SA missed to seek the opinion of the EDPB or does not follow it

National Authority for Data Protection
and Freedom of Information

Urgency procedure

Supplementary to other procedures

In exceptional circumstances where there is an urgent need to protect the data subjects

Scope is limited in time (3 months) and territory (member state)

EDPB may also issue binding opinion or decision in case a competent SA has not taken an appropriate measure in a situation where there is an urgent need to act

National Authority for Data Protection
and Freedom of Information

Code of conduct and certification

Means of proper application of the GDPR and also demonstrating compliance

Code of conduct – specific rules for a group of controllers, monitoring body

Certification – criteria checked by a certification body