Document 2.1.3

THE EFFECTIVENESS OF SANCTIONING MECHANISMS FOR DATA PROTECTION INFRINGEMENTS

Component 2
Activity 2.1.3

The content of this report is the sole responsibility of Human Dynamics and can in no way be taken to reflect the views of the European Union.

Support to the Directorate for Personal Data Protection
This project is funded by the European Union.
I. INTRODUCTION

II. REVISION DIRECTIVE 95/46/EC

III. DIRECTIVE 95/46/EC

IV. SELECTED EU MS LEGISLATION CONCERNING SANCTIONS

Austria

Bulgaria

Denmark

Estonia

Finland

France

Ireland

Italy

Poland

Slovakia

Slovenia

Spain

The Czech Republic

U.K.

V. INTERESTING CASES

Google case

Facebook

Yahoo!

Support to the Directorate for Personal Data Protection

This project is funded by the European Union
Big Brother fine confirmed

VI. COMPARATIVE TABLE

VII. CONCLUSIONS

VIII. RECOMMENDATION

Support to the Directorate for Personal Data Protection

This project is funded by the European Union
I. Introduction

The new challenges to data protection (which are globalisation and the technological changes) require strong supervision by Data Protection Authorities, in more uniform and effective way. The European framework should guarantee uniform standards as for independence, and advisory role in the legislation making process and also effective powers, including imposing sanctions and fines to data controllers and processors for breaching data protection legal principles.

European legislative reform is needed to give data protection authorities an active role in procedures which lead to sanctions and compensation. Where data protection authorities have the relevant powers, they need the resources to effectively use them. The system of compensation also needs to be simplified to facilitate litigation, by measures such as lump sum compensation (where a litigant does not need to prove the nature and extent of the damage, just the violation of the law).

II. Revision Directive 95/46/EC

The new European legal framework, which was announced by the European Commission in November 2011 will require for Data Protection Authorities:

- complete institutional independence (not to be subordinated to any other government authority);
- functional independence (not to be subject to instruction by the controlled, in relation to the contents and extent of its activity);
- material independence (they should have an infrastructure which is suited to the smooth conduct of their activities, in particular adequate funding).

The European data protection authorities discussed the need to rethink the role of WP29 to ensure that national laws on supervision and enforcement are uniformly and effectively applied. The sanction and enforcement powers of the data protection authorities need to be reinforced and harmonised. This includes the need for the authorities to be given the same tools to sanction breaches and to enforce the data protection legislation:

2.5. A stronger institutional arrangement for better enforcement of data protection rules

Support to the Directorate for Personal Data Protection
This project is funded by the European Union
The implementation and enforcement of data protection principles and rules is a key element in guaranteeing respect for individuals’ rights.

In this context, the role of the Data Protection Authorities (DPAs) is essential for the enforcement of the rules on data protection. They are independent guardians of fundamental rights and freedoms with respect to the protection of personal data, upon which individuals rely to ensure the protection of their personal data and the lawfulness of processing operations. For this reason, the Commission believes that their role should be strengthened, especially having regard to the recent European Court of Justice (ECJ) case law on their independence, and they should be provided with the necessary powers and resources to properly exercise their tasks both at national level and when co-operating with each other (see recent judgements of the ECJ in case Germany and Austria).

At the same time, the Commission considers that Data Protection Authorities should strengthen their cooperation and better coordinate their activities, especially when confronted by issues which, by their nature, have a cross-border dimension. This is particularly the case where multinational enterprises are based in several Member States and are carrying out their activities in each of these countries, or where coordinated supervision with the European Data Protection Supervisor (EDPS) is required.

III. Directive 95/46/EC

In the introducing recitals Directive 95/46/EC declare that sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under Directive (recital 55).

Thus, Article 24 is relevant to this and stipulates sanctions:

“The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive”.

In decision on imposing sanction the DPDP acts fully independently. The DPDP shall take into consideration several circumstances in its decision. Full independence of the supervisory body is required with Article 28(1) of Directive.
IV. Selected EU MS legislation concerning sanctions

It is a lack of harmonization between EU Member States regarding enforcement data protection legislation including imposing sanctions. One of aims of revised Directive is also strengthen the effectiveness of sanctions system and introducing better cooperation between Data protection authorities. The EU encourages the idea that the same sanction shall be impose for the same breach of data protection legal principle within whole EU area.

Austria

Legislation: Federal Act concerning the Protection of Personal Data (DSG 2000)
Supervisory authority: Austrian Data Protection Commission (Österreichische Datenschutzkommission)

Penal Provisions

§ 51. (1) Whoever with the intention to enrich himself or a third person unlawfully or to harm someone in his entitlement guaranteed according to § 1 para 1 deliberately uses personal data that have been entrusted to or made accessible to him solely because of professional reasons, or that he has acquired illegally, for himself or makes such data available to others or publishes such data with the intention to make a profit or to harm others, despite the data subject’s interest in secrecy deserving protection, shall be punished by a court with imprisonment up to a year, unless the offence shall be subject to a more severe punishment pursuant to another provision.

Administrative Penalties

§ 52. (1) Insofar as the act does not realise the legal elements of a criminal offence subject to the jurisdiction of the courts of law and is not subject to more severe penalties according to another administrative provision, an administrative offence punishable by a fine of up to 25 000 Euro is committed by anyone who:

1. intentionally and illegally gains access to a data application or maintains an obviously illegal means of access or
2. transmits data intentionally in violation of the rules on confidentiality (§ 15), and in particular anybody who uses data entrusted to him according to § 46 and 47 for other purposes or
3. uses or fails to grant information, to rectify or erase data in violation of a final judicial decision or ruling, 
4. intentionally erases data in violation of § 26 para. 7;
5. by pretending incorrect facts intentionally obtains data according to § 48a.

(2) Insofar as the act does not realise the legal elements of a criminal offence subject to the jurisdiction of the courts of law, an administrative offence punishable by a fine of up to 10 000 Euro is committed by anyone who
1. collects, processes and transmits data without having fulfilled his obligation to notification according to §§ 17 or 50c or operates a data application in a manner deviating from the notification.
2. engages in transborder data transmissions or commitings without the necessary permit of the Data Protection Commission according to § 13 para 1 or
3. violates declarations given according to § 13 para 2 sub-para. 2, § 19 or 50c para 1 or conditions imposed by the Data Protection Commission according to § 13 para 1 or § 21 para 2 or
4. violates his obligations of disclosure and information according tosects. 23, 24, 25 and 50d or
5. grossly neglects the required data security measures according to § 14 or
6. disregards the safety measures required according to § 50a para 7 and § 50b para 1 or
7. does not delete data after expiring of the period provided for in § 50b para 2 for deletion.

(2a) To the extent the act does not constitute a criminal offence within the jurisdiction of the courts or is punishable under other administrative penal regulations, who, contrary to §§ 26, 27 or 28, does not in time give information on, corrects or deletes data, commits an administrative offence to be punished with a **fine up to € 500**.

(3) Attempts shall be punished.

(4) Data media or programs as well as picture transmitting or recording devices can be confiscated, if they are linked to an administrative offence according to para. 1 and 2.

(5) The District Administrative Authority at the controllers (processors) domicile or seat shall be the competent authority for decisions according to para. 1 to 4. If there is no domicile or seat in Austria, the District Administrative Authority at the seat of the Data Protection Commission shall be competent.

**Bulgaria**


**Supervisory authority:** Commission for Personal Data Protection (Комисията за защита на личните данни)
Chapter Eight  
ADMINISTRATIVE PENAL PROVISIONS

Art. 42

(1) The personal data controller shall be imposed a fine or a property sanction in the amount of **BGN 10 000 to BGN 100 000** for violations of the provisions of Art. 2, para. (2) and Art. 4,

(2) The data controller shall be imposed a fine or a property sanction in the amount of **BGN 10 000 to BGN 100 000** for violations of the provisions of Art. 5.

(3) The data controller shall be imposed a fine or a property sanction in the amount of **BGN 2 000 to BGN 20 000** for violations of the provisions of Art. 19, para. (1) and Art. 20, para. (1).

(4) A data controller who has failed to meet its obligation to register as provided for in Art. 17, para. (1), shall be imposed a fine or a property sanction in the amount of **BGN 1 000 to BGN 10 000**.

(5) (new - SG 91/06) A data controller who has started data processing in violation of Art. 17b, para. (4), shall be imposed a fine or property sanction in the amount of **BGN 2 000 to BGN 20 000**.

(6) A data controller, who has failed to meet his/her obligations as provided for in Art. 22, para.s (1) and (2), shall be imposed a fine or property sanction in the amount of **BGN 2 000 to BGN 20 000**.

(7) A data controller who does not issue an administrative act concerning the application under Art. 29 within the term, shall be imposed a fine or a property sanction in the amount of **BGN 1 000 to BGN 20 000**, unless he/she is a subject to a more severe sanction.

(8) Persons who refuse to cooperate with the Commission with regard to its control powers, shall be imposed a fine or a property sanction in the amount of **BGN 1 000 to BGN 10 000**.

(9) The guilty persons shall be imposed a fine or a property sanction in the amount of **BGN 500 to BGN 5 000** for any other violation of the provisions of this Law.

**Art. 42a**

In cases of violations under this Law committed as repeated violations, a fine or property sanction shall be imposed in an amount **twice higher** than the initially imposed penalty.

**Art. 43**

(1) The acts of determining administrative violations shall be constituted by a member of the Commission for Personal Data Protection or by officials authorized by the Commission.

(2) The penal decrees shall be issued by the President of the Commission for Personal Data Protection.
(3) Property sanctions and fines imposed by penal decrees in force, shall be collected under the order of the Code of Tax and Social Security.

(4) The determination of the violations, the issuance, the appeal and the execution of the penal decrees shall be carried out in compliance with the Administrative Violations and Sanctions Act.

Note: 1 € = 1.956 BGN

**Denmark**

**Legislation:** Act on Processing of Personal Data (No.429 of 31 May 2000), amended several times, most recently 1 July 2007

**Data protection authority:** Datatilsynet (The Danish Data Protection Agency)

Any person or legal entity committing an offence - fine or imprisonment - DPA cannot impose sanctions; they request the Danish Public Prosecution Office to instigate proceedings.

**Highest fine to date:** £2,500

**No prison sentences to date.**

The DPA can issue an enforcement notice or go straight to an offence and pass the case to the public prosecutor. It depends on the case. This is for private sector only.

For the public sector, they inform the relevant minister or head of the municipality. They cannot fine or give prison sentences to public authorities.

Once a case is with the public prosecutor it becomes like any other criminal case, and the court decides on the fine and or other sanctions.

**Audit/Inspection**

The DPA can audit public or private sector organisations without notifying them in advance and they don't need the organisation's permission.

The DPA can only audit private sector organisations where they are processing as covered by s50 of their law (the organisation is notified or they are processing data they need an authorisation for).

Generally, the DPA do inform the organisation in advance of an audit / inspection by sending a letter, and they usually ask for information in advance of the audit, such as the security description.

If there are problems found, they ask the company to send them any information / notify and so on. When the DPA is satisfied, they send a final letter to sum up
the case and close it. They sometimes have to notify the police if they find serious problems during the inspection.

The DPA reports to Parliament every year and this includes the number of inspections done. Their target is 60 a year and they average 60 to 70.

**Estonia**

**Legislation:** Personal Data Protection Act 2003  
**Data protection authority:** Andmekaitse Inspektsioon (Estonian Data Protection Inspectorate)

42. Violation of requirements of this Act

(1) Violation of the obligation to register the processing of sensitive personal data, violation of the requirements regarding security measures to protect personal data or violation of other requirements for the processing of personal data is punishable by a fine of up to 300 fine units.

(2) The same act, if committed by a legal person, is punishable by a fine of up to 50 000 kroons.

(3) The provisions of the General Part of the Penal Code (RT I 2001, 61, 364; 2002, 82, 489; 86, 504; 105, 612; 2003, 4, 22) and the Code of Misdemeanour Procedure (RT I 2002, 50, 313; 110, 654) apply to the misdemeanours provided for in this section.

(4) The Data Protection Inspectorate is the extra-judicial body which conducts proceedings in matters of misdemeanours provided for in this section.

**Finland**

**Legislation:** Personal Data Act (523/1999) as amended of 2000  
**Supervisory authority:** The Office of the Data Protection Ombudsman (Tietosuojavaltuutetun Toimisto)

Finland hasn’t separate provisions relate to sanctions and fines. The Ombudsman shall proceed it in accordance with Penal Code of Finland.

Section 46 — Threat of a fine

The Data Protection Ombudsman may impose a threat of a fine, in accordance with the Act on Threats of a Fine (1113/1990), in order to reinforce the duty to provide access to data, as referred to in section 39(1) and 39(3), and a decision made on the basis of section 40(2); the Data Protection Board may do likewise in relation to the duty to provide access to data, as referred to in section 39(1), and a decision made on the basis section 44.
Section 48 — Penal provisions

The penalty for a personal data offence is provided in chapter 38, section 9 of the Penal Code (39/1889) and for breaking into a personal data file in chapter 38, section 8 of the Penal Code. The penalty for a violation of the secrecy obligation referred to in section 33 is provided in chapter 38, section 1 or 2 of the Penal Code, unless the act is punishable under chapter 40, section 5 of the Penal Code or a more severe penalty is provided in another Act.

France

Supervisory authority: Commission nationale de l’informatique et des libertés (CNIL)

The “Commission nationale de l’informatique et des libertés” (CNIL) has following types of sanctions: warnings, formal demands, injunction to cease processing, financial sanctions up to €150,000 for first breach and up to €300,000 for further breaches and Criminal sanctions up to max 5 years in prison and fines from €15,000 to €300,000.

In accordance with the Law, the CNIL may issue a warning to a data controller who does not comply with obligations resulting from the Law. Imposing sanctions which CNIL may impose to data controller is stipulated in Chapter VII of the Law. The CNIL may also order the data controller to cease the breach within a time limit that it determines. If data controller does not comply with this order, the commission may impose the following penalties on him, after fair proceedings:
- a financial penalty, within the conditions provided for in Article 47 of the Law, except in cases where the processing is carried out by the State;
- an injunction to stop processing, where the provisions of Article 22 apply to it, or a withdrawal of the authorisation given by virtue of Article 25.

The CNIL can issue warnings and compliance notices (like enforcement notices). Non-compliance with these can result in financial sanctions (but not the public sector) of up to €150,000, then up to €300,000 for subsequent offences, or 5% of turnover - up to a max of €300,000. Or they can issue an order to stop processing. Fines only follow the issuing of a notice. Serious cases can be referred to the public prosecutor, although this rarely happens. It is usually in cases where the CNIL does not have the power to carry out the necessary investigations. The courts can issue fines or prison terms - up to 5 years in prison and fines of up to €300,000.

In emergency cases they can interrupt or block processing for up to 3 months, or inform the Prime Minister if public security files are involved. The President can
ask a judge to order any necessary security measures in serious cases. They can also withdraw their authorisation.

**Audit/Inspection**

The DPA can access all professional premises, request and copy all necessary documents, access all IT systems, and request transcriptions of data. They used to inform companies of inspections but this didn’t work very well, so now most are on-the-spot inspections. They have to inform the local judge in case they are refused access to premises, in which case the judge can order the company to let them in.

Non-compliance with report recommendations can lead to the threat of financial sanctions, or they can refer the case to the public prosecutor.

The financial penalties shall be collected as State debts, other than taxes and income from State assets.

**Ireland**

**Legislation:** Data Protection Act 1988, modified by Data Protection (Amendment) Act 2003 of 1 July 2003

**Data protection authority:** Data Protection Commissioner

(An Coimisinéir Cosanta Sonraí)

Breaches may incur civil liability or criminal sanctions, including fines.

Blagging offence - €3,000 - not prosecuted anyone yet

Failure to comply with notices - €3,000

Prosecution on indictment - up to €100,000 - never used yet, not clear under what circumstances it could be used.

No prison sanctions

Breach of principle is not an offence, may result in enforcement notice.

The Ireland DPA has the same powers as the U.K. ICO in terms of serving information and enforcement notices. They also have a prohibition notice relating to international transfers.

**Audit/inspection**

They have the power under s10 of their law to audit for practice and compliance with the Act. They don’t tend to use this power. In they do, they contact the company and tell them they will audit on a particular date. The company has some leeway to change the date, but not much.

Instead they use (and increasingly so) the power under s24 to be able to enter any premises at any time without notice. It is a power of entry and to copy
information. They can turn up anywhere at any time and look at personal data processed or information relating to the processing. A failure by an organisation to cooperate is an offence and they are cautioned and possibly prosecuted. They do not take the police with them, it has not been needed so far, but they could ask if they wanted to.

They are increasingly using this power with organisations involved in mobile marketing. Under the legislation that has enacted the e-privacy directive they have the power to prosecute any offences under that law and to impose fines of €3,000 for every message sent or every failure to comply. The court can also order the deletion of a database and there is draft legislation at the moment to increase the fine to €5,000; and a maximum of 10% of a company's turnover, or €4 million. Some large-scale prosecutions are expected.

The Director of public prosecutions carries out the sanctions. The DPA makes the case and takes it to court. They recommend the fine or other sanction (measures to be taken and so on). The court decides ultimately, and may levy fines of less than the DPA recommended.

Civil sanctions Where a person suffers damage as a result of a failure by a data controller or data processor to meet their data protection obligations, then the data controller or data processor may be subject to civil sanctions by the person affected. Ordinarily, the "injury" suffered by a data subject will be damage to his or her reputation, possible financial loss and mental distress. The data subject concerned may have adequate remedies under the existing law (defamation where appropriate, breach of confidentiality and so on, but, more frequently perhaps, in negligence because in some cases a data controller or a data processor would owe a duty of care to data subjects about whom data are being kept or processed - a duty to see that damage is not caused to them by negligent handling of the data in question). In so far as a data controller or data processor may not be subject to this duty of care, section 7 of the Data Protection Acts remedies this by ensuring that such a duty will be implied in all cases where personal data are kept or processed.

If the commission of an offence under the Data Protection Acts also involves violence - for example, if an "authorised officer" is assaulted in trying to gain access to the premises under section 24 - then the offender can be proceeded against for assault and be liable to imprisonment.

Summary proceedings for an offence under S.I. 535 of 2003, as amended by S.I. 526 of 2008, may be brought and prosecuted by the Commissioner. Each call or message can attract a fine of up to €5000 on summary conviction. If convicted on
indictment, the fines range from €50,000 for a natural person to €250,000 or 10% of turnover if the offender is a body corporate.

**Italy**

**Legislation:** Protection of individuals and other subjects with regard to the processing of personal data Act - replaced by the Consolidation Act regarding the processing of personal data.

**Data protection authority:** Garante Per la Protezione Dei Dati Personalì (Il Garante)

The administrative penalties scheme under the Italian Data Protection Code (Legislative Decree 30 June 2003 n. 196) has recently been substantially amended.

**Criminal, civil and administrative sanctions**

The Garante can impose administrative sanctions - fines - for not providing data subject with info subject to information notice or for non-notification. Up to 3 years in prison and publication of judgement for unlawful processing, if damage occurs; false notification; and failure to adopt and implement the required security measures. The DPA (Garante) put together a case and if there is evidence of criminal conduct, they pass the information on to the police and judicial authorities. The judicial authorities carry out any investigations. They can then impose sanctions including up to 3 years in prison, as described above. The DPA can ask an organisation for information and documents and the organisation has to reply. If they don't, they are liable to a fine or criminal punishment. Fines are from €4,000 to €24,000. Criminal punishments are used for repeat offenders or for providing false information. The DPA can issue the order to pay a fine.

**Audit/Inspection**

The DPA targets organisations or sectors based on intelligence from complaints or by acting on their own initiative and according to their priorities. If these paper inspections do not yield enough information, they can carry out on the spot inspections. In 2006 they carried out 350 inspections with 158 administrative breaches found and 11 cases referred to the judiciary. Article 44 of the Decree, dated 18 December 2008, no. 207 (published in the Italian Official Gazette no. 304 dated 31 December 2008) tightens the administrative penalties under the Italian DP Code.
1. by doubling the amounts of the original sanctions (in some cases the amount of the minimum and maximum fines have more than doubled);
2. by imposing additional administrative penalties in case of violation of certain specific requirements of the Italian Data Protection Code; and
3. by introducing new sanctions for new offences.

It is likely that the administrative penalties scheme has been revised. The experience of other Italian regulatory sectors (where an increase in sanctions has increased market operators’ focus on their legal obligations and led to a reduction in the number of violations) has most likely led to the decision to implement a more severe punishment scheme in the data protection sector, as part of the Italian Data Protection Authority’s plan to ensure that controllers are more focused on data protection and take more responsibility.

1. **Failure to provide information, or provision of inadequate information, to the data subject (Article 161 of the Italian DP Code).**

   The fine for failure to provide an information notice (or adequate information) to the data subject, will now be between 6,000 and 30,000 EUR (the original fine was in the region of 3,000-18,000 EUR);

2. **Failure to comply with requirements in case of assignment of data or other provisions on processing of data (para 1 of Article 162 of the Italian DP Code).**

   The fine for failure to comply with these requirements will be from 10,000 to 60,000 EUR (the original fine was 5,000- 30,000 EUR);

3. **Unlawful disclosure of medical data (para 2 of Article 162 of the Italian DP Code)**

   The fine for failure to comply with the obligation only to disclose medical data to the data subject through a physician expressly identified by the data subject or by the controller will be from 1,000 to 6,000 EUR (instead of the original amount of 500-3,000 EUR);

4. **Failure to notify or incomplete notification (Article 163 of the Italian D Code)**

   The fine for failure to comply with a notification requirement on time will be between 20,000 and 120,000 EUR (instead of the original amount of 10,000-60,000 EUR);
5. **Failure to provide the Garante with requested information/documents (Article 164 of the Italian DP Code)**

The fine will be 10,000-60,000 EUR (instead of the original amount of 4,000-24,000 EUR) where the controller fails to provide the Garante with information or documents formally requested by the Authority;

6. **Minor violations and more serious violations (new Article 164-bis of the Italian DP Code)**

In contrast to the original set of rules concerning administrative fines, according to the new penalties scheme, a reduction of two fifths can now be applied to fines where the violations are minor, considering the financial or social nature of the processing. This applies to the fines above.

However, a fine of 50,000-300,000 EUR will be imposed where:

- there are more serious violations of the provisions (Articles 161, 162 para.1, 162 para 2-bis, 162 para 2-ter, and 163);
- more than one of the provisions were breached; and
- the processing relates to a database which is significant in size or content.

A company cannot benefit from a removal of the penalty in return for payment of a reduced amount (i.e. “*pagamento in misura ridotta*”).

In more serious cases, in particular whenever the damage suffered is more substantial or if the violation concerns several data subjects, the upper and lower thresholds of the applicable fines under Articles 161 to 164-bis shall be doubled. Additionally, the fines under Articles 161 to 164-bis may be increased by up to four times if they prove ineffective on account of the offender’s financial status.

7. **Failure to implement minimum security measures under Article 33 of the Italian DP Code**

The original penalty (Article 169 of the Italian DP Code) for failure to implement minimum security measures was imprisonment of up to 2 years (unless within the Authority’s deadline, the controller complies with any conditions imposed by the Garante as a result of administrative proceedings which established that the minimum security measures had not been implemented) **OR** the payment of a fine of 10,000-50,000 EUR.

Under the new administrative penalties scheme (para 2-bis of Article 162, and Article 169 of the Italian DP Code) failure to comply with this requirement will
now be subject to **both** penalties, i.e. imprisonment of up to 2 years (unless, within the Authority's deadline, the controller complies with any prescriptions imposed by the Garante as a result of administrative proceedings and payment of an increased fine now 20,000-120,000 EUR without the possibility of removing the charge by payment of some of the fine.

8. **A significant change has also been introduced by Article 44 of the d.l. 207/2008**

Under the new provisions of para 2-bis of Article 162 of the Italian DP Code, whenever personal data are processed without the consent of the data subject (including, without limitation, processing of traffic data, processing of phone numbers collected on phone directories, White Pages, processing of sensitive data, etc.) the offender shall be subject to a criminal sanction (i.e. imprisonment for a period of time depending on the kind of processing and/or of the type of data) and to a new administrative fine of between 20,000-120,000 EUR;

9. **A specific sanction has now been introduced**

Where there is a failure to comply with measures set forth under general prescriptions of the Garante or in case of failure to follow a prohibition by the Garante on further processing personal data (e.g. data collected unlawfully) (para. 2-ter of Article 162 of the Italian DP Code): in this case the fine will be in the range of 30,000 to 180,000 EUR.

Finally, in all violations under Articles 161-164-bis, the offender shall be responsible for publishing the Authority's order in the newspapers identified in the decision and for bearing the relevant costs.

D.L. 207/2008, Article 44 has also amended the amount of fines provided under para 1 of Article 62 of the Italian Consumers Code (D.lgs. 206 dated 6 September 2005). Therefore, where there is failure to comply with the provisions on conclusion of a contract with the consumers (including the use of distance communication technology without the consumer's consent) the professional can be sanctioned with a fine of between 3,000 to 18,000 EUR (instead of 516 - 5,165 EUR).
**Poland**

**Legislation:** The Act on the Protection of Personal Data (of 29 August 1997, as amended on 2010)

**Supervisory Authority:** The Inspector General for the Protection of Personal Data (Biuro Generalnego Inspektora Ochrony Danych Osobowych)

The Polish DPA is able to impose fines 10,000 PLN on a natural person, and PLN 50,000 on a legal person. If numerous fines are imposed in the course of one enforcement proceeding, the total amount of fines may not exceed PLN 50,000 to natural persons and PLN 200,000 with regard to legal persons.

Note: 1€ = 3,96 PLN

**Slovakia**


**Supervisory Authority:** The Office for Personal Data Protection (Úrad pre ochranu osobných údajov)

Chapter 4 - SANCTIONS FOR THE ACT VIOLATION

Section 49 Administrative Offences

(1) The Office may impose a fine in the amount from SKK 50,000 to SKK 10,000,000 to the controller or the processor who a) failed to fulfil or breached some obligations stipulated in the Law, or failed to take due technical, organisational and personal measures adequate to the manner of the processing or failed to prove

(2) The Office may impose a fine in the amount from SKK 50,000 to SKK 5,000,000 to the controller or the processor who failed to fulfil or breached other stipulated in Section 13, or failed to provide, upon request of the Office, execution of an audit of the filing system’s security or provided execution of the audit of the filing system’s security contrary to Act or transferred personal data to third countries contrary to Section 23, or processes or processed personal data contrary to any of the conditions stipulated in the Law.

(3) The Office may impose a fine in the amount from SKK 30,000 to 3,000,000 to the controller who failed to fulfil the obligation of special registration of the filing system or failed to fulfil any of the obligations connected with the special registration arising from this Law or failed to authorize a personal data protection official in writing for execution of internal supervision of personal data protection or cannot credibly prove his authorization in writing, or failed to
provide professional training of the personal data protection official in accordance with this Act.

(4) The Office may impose a fine in the amount from SKK 10,000 to SKK 1,000,000 to the controller who failed to fulfil the obligation to notify of rectification or destruction of personal data.

(5) The Office may impose a fine up to the amount of SKK 100,000 to the person who provides false personal data, breaches the obligation to maintain secrecy about personal data.

(6) The Office may impose a fine under Paragraphs 1 to 4 and under Section 50 repeatedly, provided that the obligation was not fulfilled in a determined time limit.

(7) In the imposition of fines, the gravity, time of duration and consequences of the illegal conduct shall be taken into account above all.

(8) Proceeds from the fines shall constitute an income of the State budget.

**Section 50 Disciplinary Fines**

(1) The Office may impose a disciplinary fine to the controller or to the processor:

    a) up to the amount of SKK 50,000, provided that he fails to provide adequate conditions for execution of the inspection,
    b) up to the amount of SKK 500,000, provided that he frustrates execution of the inspection; if the controller or the processor proves that frustration of execution of the inspection was caused by the entitled person, his liability shall be restricted and the entitled person shall also become liable,
    c) up to the amount of SKK 1,000,000, provided that he failed to make public at all, or failed to make public in time, a notice designated to be made public in the mass media by the President of the Office or the chief inspector, or provided that he failed to make the above notice public in the determined form or in the determined mass medium, or provided that he failed to adhere to the determined contents of this notice under Section 48; the fine may be imposed repeatedly until fulfilment of the obligation,
    d) up to the amount of SKK 2,000,000, provided that he failed to provide the Office with the cooperation under Section 44 or failed to satisfy the requests of the Office or failed to notify the Office in a determined time limit under Section 46.

(2) Disciplinary fine may be imposed within one year from the day when the obligation was breached.
Note: 1 € = 30.13 SKK

**Slovenia**

**Legislation:** Personal Data Protection Act 2007  
**Data protection authority:** Information Commissioner (Informacijski Pooblaščenec)

Information commissioner (DPA) in the Republic in Slovenia is also an authority for decision-making on offences (the misdemeanour authority), under the Personal Data Protection Act, Minor Offences Act and some other legislation (Media Act)

**Criminal provisions in the Personal Data Protection Act**, Official consolidated text (ZVOP-1 2004 and ZVOP 1A 2007)

**General violations of the provisions of this Act** (Article 91)

1) A fine of **4,170 to 12,510** euros shall be imposed **on a legal person, sole trader or individual independently performing an activity**:
   1. when processing personal data without the need for a basis in law or in the personal consent of the individual (Article 8), or when breaching;
   2. where individual tasks related to the processing of personal data entrusted to another person without a contract in accordance with Article11;
   3. if the process sensitive personal data contrary to the Article 13;
   4. if they automated processes personal data in contravention of the Article15;
   5. when collecting personal information for purposes other than those specified and legitimate, or if they are further processed in contravention of Article16;  

   (......)

2) A fine of **830 to 2,080** euros shall be imposed for an offence under the preceding paragraph **on the responsible person**, sole trader or individual independently performing an activity.

3) A fine of **830 to 2,080** euros shall be imposed upon **the responsible person of a state agency or local authority** who commits an act of the first paragraph of this article.

4) A fine from **200 to 830** euros shall be imposed **on an individual** who commits the offence in the first paragraph of this article.

**Violation of the provisions of the contract processing** (Article 92)
1) A fine of **4170 to 12,510** euros shall be imposed on a legal person, sole trader or individual independently performing an activity if it exceeded the powers contained in the contract referred to in second paragraph of the Article 11 or return of personal data in accordance with Article 11.

2) A fine of **830 to 2,080** euros shall be imposed for an offence under the preceding paragraph on the responsible person, sole trader or individual independently performing an activity.

3) A fine of **830 to 2,080** euros shall be imposed upon the responsible person of a state agency or local authority who commits an act of the first paragraph of this article.

4) A fine from **200 to 830** euros shall be imposed on an individual who commits the offence in the first paragraph of this article.

**Violation of the provisions of protection of personal data (Article 93).**

1) A fine of **4170 to 12,510** euros shall be imposed on a legal person, sole trader or individual independently performing an activity which, in accordance with this Act to process personal data and does not ensure the security of personal data.

2) A fine of **830 to 1,250** euros shall be imposed for an offence under the preceding paragraph on the responsible person, sole trader or individual independently performing an activity.

3) A fine of **830 to 1,250** euros shall be imposed upon the responsible person of a state agency or local authority who commits an act of the first paragraph of this article.

4) A fine from **200 to 830** euros shall be imposed on an individual who commits the offence in the first paragraph of this article.

**Violation of the provisions on direct marketing (Article 94)**

1) A fine from **2,080 to 4,170** euros shall be imposed on a legal person, sole trader or individual independently performing an activity which, in accordance with this Act process personal data for direct marketing purposes and is not complying with the Article 73 of this Act.

2) A fine from **410 to 1,250** euros shall be imposed for an offence under the preceding paragraph on the responsible person, sole trader or individual independently performing an activity.

3) A fine from **200 to 830** euros shall be imposed on an individual who commits the offence in the first paragraph of this article.

**Violation of the general provisions on video surveillance (Article 95).**
1) A fine of **4,170 to 12,510 euros** shall be imposed on a **legal person, sole trader or individual independently performing an activity**:
   1. if it fails to publish notice in the manner specified in the second paragraph of Article 7;
   2. if the notice does not contain information from the third paragraph of the Article 74;
   3. if it does not protect a video monitoring system, which implements the video surveillance in contravention of the fifth paragraph of the Article 74th.

2) A fine of **830 to 1,250 euros** shall be imposed for an offence under the preceding paragraph on the **responsible person, sole trader or individual independently performing an activity**.

3) A fine of **830 to 1,250 euros** shall be imposed upon the **responsible person of a state agency or local authority** who commits an act of the first paragraph of this article.

4) A fine from **200 to 830 euros** shall be imposed on an individual who commits the offence in the first paragraph of this article.

Violation of the provisions on video surveillance of access to official business or commercial premises  (Article 96)

1) A fine of **4170 to 12,510 euros** shall be imposed on a **legal person, sole trader or individual independently performing an activity**:
   1. if video surveillance conducted without a reasoned written decision whether or not other legal bases in the first paragraph of the Article 75;
   2. if video surveillance conducted by carrying out the shooting inside the residential buildings that have no impact on access to their premises or videos entrances to apartments (the second paragraph of the Article 75);
   3. if a written notification to employees (third paragraph of the Article 75);
   4. if personal data held in contravention of the fifth paragraph of the Article 75.

2) A fine of **830 to 1,250 euros** shall be imposed for an offence under the preceding paragraph on the **responsible person, sole trader or individual independently performing an activity**.

3) A fine of **830 to 1,250 euros** shall be imposed upon the **responsible person of a state agency or local authority** who commits an act of the first paragraph of this article.

4) A fine from **200 to 830 euros** shall be imposed on an individual who commits the offence in the first paragraph of this article.

Violation of the provisions on video surveillance  (Article 97)
1) A fine from **2,080 to 8,340 euros** shall be imposed on a **legal person, sole trader or individual independently performing an activity** that video surveillance in multi-dwelling buildings.

2) A fine from **410 to 1,250 euros** shall be imposed for an offence under the preceding paragraph on the **responsible person, sole trader or individual independently performing such activity**.

3) A fine of **830 to 1,250 euros** shall be imposed upon the **responsible person of a state agency or local authority** who commits an act of the first paragraph of this article.

4) A fine from **200 to 410 euros** shall be imposed on an **individual** who commits the offence in the first paragraph of this article.

### Violation of the provisions on video surveillance in work place (Article 98)

1) A fine of **4,170 to 12,510 euros** shall be imposed on a legal person, sole trader or individual independently performing an activity carried out video surveillance in work areas contrary to the provision of the Article 77.

2) A fine from **1,250 to 2,080 euros** shall be imposed for an offence under the preceding paragraph on the **responsible person, sole trader or individual independently performing an activity**.

3) A fine from **1,250 to 2,080 euros** shall be imposed upon the **responsible person of a state agency or local authority** who commits an act of the first paragraph of this article.

4) A fine of **830 to 1,200 euros** shall be imposed on an **individual** who commits the offence in the first paragraph of this article.

### Violation of the provisions on biometrics in the public sector (Article 99)

1) A fine from **4,170 to 12,510 euros** shall be imposed upon a **public sector** that performs biometric measures contrary to the Article 79.

2) A fine from **1,250 to 2,080 euros** shall be imposed for an offence under the preceding paragraph on the **responsible person of the public sector**.

3) A fine from **1,250 to 2,080 euros** shall be imposed for an offence under the first paragraph of this Article the **responsible person state agency or local authority** who commits an act of the first paragraph of this article.

### Violation of the provisions on biometrics in the private sector (Article 100)
1) A fine of **4170 to 12,510 euros** shall be imposed on a legal person, sole trader or individual independently performing an activity that performs biometric measures contrary to the Article 80.

2) A fine from **1,250 to 2,080 euros** shall be imposed for an offence under the preceding paragraph on the responsible person, sole trader or individual independently performing an activity.

**Violation of the provisions on record entries and exits** (Article 101).

1) A fine from **2,080 to 4,170 euros** shall be imposed on a legal person, sole trader or individual independently performing an activity:
   1. using a record of entries and exits as the official record, contrary to paragraph 82nd Article;
   2. acting contrary to the fourth paragraph of the Article82.

2) A fine from **200 to 830 euros** shall be imposed on the responsible person, a sole proprietor or an individual who is self-employed person who commits an offence under the preceding paragraph.

3) A fine from **200 to 830 euros** shall be imposed upon the person responsible state agency or local authority who commits a misdemeanour of the first paragraph of this article.

4) A fine from **200 to 410 euros** shall be imposed upon an individual who commits an offence under the first paragraph of this article.

**Violation of the provisions on the integration of databases** (Article 102)

(1) A fine of **830 to 2,080 euros** shall be imposed upon the responsible person of a state authority or local authority, which connects to a collection of personal data contrary to the third paragraph of the Article84.

(2) A fine of **830 to 2,080 euros** shall be imposed upon the responsible person of a state authority or local authority, which connects personal database of criminal records and violation records with other collections of personal data or link the personal database of criminal records by filing data in violation of records (Article 85).

**Violation of provisions relating to professional supervision** (Article 103)

1) A fine from **4,170 to 12,510 euros** shall be imposed on a legal person:
   1. if act under peer supervision contrary to the second paragraph of the Article;
   2. if it does not make the official record or other official record.

2) A fine of **830 to 1,250 euros** shall be imposed for an offence under the preceding paragraph on the responsible person.
3) A fine of **830 to 1,250 euros** shall be imposed upon the **responsible person of a state agency or local community** who commits the offence in the first paragraph of this article.

4) A fine from **200 to 830 euros** shall be imposed on an **individual** who commits the offence in the first paragraph of this article.

* * *

In 2009 163 violation procedures were initiated as a consequence of violations of the provisions of the Personal Data Protection Act; these were namely: 41 procedures against public sector entities, 70 against legal entities in the private sector, and 52 procedures against individual persons. Violation proceedings are considered in accordance with the Personal Data Protection Act.

As a consequence of established violations, the Information Commissioner issued: 59 warnings, 93 decisions regarding violations (encompassing 67 cautions); as well as 26 fines and 12 payment orders.

**Penalties for violation under the Minor Offences Act**

For the offences committed to the terms of the Minor Offences Act, the misdemeanor authority impose prescribed penalty or warning. Under conditions and in the manner provided by this Act, the misdemeanor authority may, instead of introducing the procedure of the offence, give the offender a warning. Property advantage can also be taken away, gained with offence.

For violations in the field of competition may be a legal person, sole trader or individual independently performing an activity, the law prescribes a fine of up to ten per cent of their turnover or their turnover with companies in the group in the previous financial year. (Article 4 of the Minor Offences Act).

The misdemeanor authority conducting the proceedings on the offence may set the amount for the property advantages withdrawal exceptionally by free deliberation, if its learning would be connected with disproportionate hardship or if procedure would drag on because of this too much. (Article 191 of the Minor Offences Act)

Withdrawal of property advantage is pronounced with decree about offence. Property advantage must be stated in decree and monetary amount to be taken away thereof.

In 2009, the Information Commissioner imposed it highest fine to date; this was in relation to two insurance companies as a consequence of the illegal processing
of personal data. The proceedings established that personal data pertaining to 2,382 former insured persons had been transferred from one insurance company to the other without legal basis or the personal consent of the individuals concerned; the data thus transferred was then used in direct marketing. The Information Commissioner imposed a EUR 112,590 fine on the insurance company for the illegal transmission and non-traceable dissemination of personal data pertaining to 26 individuals, in relation to whom firm evidence had been provided; a EUR 20,000 fine was imposed on the responsible individual. The recipient insurance company received a fine of EUR 108,420 as a consequence of illegally processing personal data pertaining to the formerly insured persons; the responsible individual at the second company also received a fine of EUR 20,000. These are the highest ever fines handed down by Slovenia’s Information Commissioner.

**Spain**

**Legislation:** Ley orgánica 15/1999 (13 December 1999), de Proteccion de Datos de Caracter Personal

**Data protection authority:** Agencia Espanola De Proteccion de Datos (Spanish Agency for Data Protection) (AEDP)

The AEPD has supervisory responsibilities for all issues related to the protection of personal information in the private sector and public sector (except local public sector in Madrid, Cataluna and the Basque Country). The Spanish Data Protection Agency (AEPD) now has a new penalty regime after reform to the country’s Data Protection Act (DPA) came into force on 6 March 2011.

The reform lowered some fines but the aim is not the reduction of the fines per se. The reform intention was to give the Spanish Data Protection Authority (AEPD) flexibility to better adopt the fines in accordance with circumstances of the breach of the law and of the offender. The sanctions for minor infringements are now more proportionate to the real damage caused by the infringement. The AEPD may take into account several factors when determining the level of fines. These factors include the size and capacity of the business of the offender and any measures which the offender implemented in order to avoid or rectify the data breach.

The fines that can be imposed for 'minor infringements' now range from €900 to €40,000. Prior to the reform, the fines that could be imposed ranged from €601.01 to €60,101.01.

---

1 Published in Boletín Official del Estado, No.55, 5 March 2011
2 AEPD – Agencia Española de Protección de Datos
Additionally, the minimum sanction for 'serious infringements' was lowered from € 60,101 to € 40,000. A further major change brought about by the reform is the reclassification of 'disclosure of sensitive data' as a 'serious infringement' - previously any disclosure of personal data would fall under the category of a 'very serious infringement', with fines ranging from € 300,000 to € 600,000.

Because the agency has the power to impose sanctions, it must guarantee due process to all parties. In this respect they have a number of powers available to them. They are able to:

(i) Request that the data controller under investigation voluntarily submits information.
(ii) Inspect organisations in situ – failure to assist the Agency is a serious infringement.
(iii) The Agency may lawfully impose fines on the data controller (private sector only) if violations in respect of the data protection legislation are discovered.
(iv) As a preventative measure they may block or stop processing of personal information.

Sanctions (fines) may be imposed following inspection and investigation. Sanctions are imposed in accordance with a sliding scale dependent upon the seriousness of the infringement. Very serious violations may incur fines up to 600,000 Euros. Examples of very serious violations are:

(i) Unauthorised transfer of data.

(ii) Unauthorised processing of specially protected data (medical, racial, sexual, ideological)
(iii) Fraudulent collection of data.
(iv) Systematic violations.

Serious violations may incur fines of up to 300,000 Euros. Examples of serious violations are as follows:

(i) Failure to maintain accuracy.
(ii) Failure to provide security measures.
(iii) Failure to register or notify as required.
(iv) Creation of data files without consent.
(v) Active refusal of rights.
(vi) Obstruction of investigation.

Audit/Inspection
The AEPD have the power to inspect/audit without the consent of the data controller. Failure to collaborate in an inspection is a serious violation which may lead to a fine being imposed of up to 300,000 Euros.

In the case of infringement of data protection law by public sector organisations fines are not imposed but public warning are issued which may lead to disciplinary proceedings against individuals.

**The Czech Republic**

**Legislation:** The Law on Personal Data Protection (as amended)

**Data protection authority:** The Office for Personal Data Protection (Úřad pro ochranu osobních údajů) (ÚOOÚ)

The penalties are divided into two categories: If the Law is violating by natural person the sanction is limited up to 5M CZK (approx. € 206,000). The level of fine is flexible in accordance which obligation has been violated and other circumstances.

The second category of sanction relates to legal persons. Here this sanction may reach up 10M CZK (approx. € 415,000).

The fines are imposed by the Data Protection Office and are enforced by the locally competent regional financial authority pursuant to special Act. The revenue from fines shall be an income of the state budget.

**U.K.**

**Legislation:** Data Protection Act 1998

**Data protection authority:** The Information Commissioner’s Office (ICO)

The U.K. sanctions regime until 2010 was that following breach of a data protection principle, an organisation may be invited by the ICO to sign a formal undertaking, wherein the CEO of the organisation undertakes to put certain measures in place in order to avoid a similar data protection failure in future. This undertaking has been published on the ICO website and, although most undertakings do not contain deadlines, it is possible for the ICO to provide a deadline for those measures to be introduced (for example, for breach of the security principle, a common undertaking is for the organisation to ensure that computers are encrypted with encryption software meeting the current standard or equivalent and, in some cases, a one to four month deadline was given for compliance.

Since 2010 some important changes in the powers of the Information Commissioner to enforce data protection legislation are in force. It's worthwhile reading for all organisations which handle personal data – information about...
identifiable, living individuals, whether staff, clients/service users, contacts or otherwise.

The main point to note is that, for the first time, a deliberate or reckless, serious failure to comply with any of the eight data protection principles in the Data Protection Act 1998 (the “DPA”) could result in a fine of up to £500,000. So, for example, a failure to put in place adequate systems to protect against the theft or loss of personal data, or to ensure that personal data is only shared with other organisations to the extent permitted by the DPA, could now result in a very substantial fine.

The amounts involved look set to persuade even the most reluctant of organisations to pay more attention to data protection compliance. If the threat of regulatory sanction still doesn’t seem real at this early stage in the new regime, it no doubt will when the first fines have been handed out. Those on the receiving end will be faced not only with paying them, but also with the negative publicity and related legal and commercial problems which a penalty of this nature could bring.

No time like the present then to have a look at your policies, procedures and practices relevant to the handling of personal data and identify (and prioritise) any issues which require to be addressed.

Monetary penalty Since 6 April 2010 the ICO has had the power to issue a formal notice requiring an organisation to pay a monetary penalty of up to £500,000. This brings the ICO’s powers in line with those already available to many national supervisory authorities around Europe. This will be imposed if an organisation has seriously contravened the data protection principles and the contravention was of a kind likely to cause substantial damage or substantial distress. In addition the contravention must either have been deliberate or the data controller must have known or ought to have known that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it. This article provides further information on monetary penalties: http://www.olswang.com/newsarticle.asp?sid=121&aid=2880

It is interesting to note that, three months after the ICO’s powers to issue this penalty came into force, no monetary fines had yet been issued. Unlike undertakings, monetary penalties do not themselves provide the data controller with any understanding of how to put matters right and so in that sense are less useful from the perspective of the Commissioner’s statutory role of promoting good practice. Clearly they play a deterrent role as part of the ICO’s “purposeful risk-based enforcement action” (as described in the Annual Report under “Our Corporate Plans”) and we look forward in due course to evidence of their usefulness in this regard.
V. Interesting cases

Google case

In May 2010, CNIL formally notified Google of the infringements and, as the company had not officially replied, on 17 March 2011, issued a 100 000 Euro fine on the company, the highest fine CNIL has applied since it received, in 2004, the power to impose financial sanctions. This record fine is for the unauthorised collection of information about the location of Wi-Fi hotspots in France by Google’s Street View cars. The fine also reflects the company’s failure to sufficiently co-operate with the CNIL in complying with France’s data protection law. Google has now apologised.

- For better or for worse, the Spanish Agency for Data Protection isn’t ready to forgive Google for collecting sensitive WiFi data along with Street View photos. Indeed, it’s moved its investigation forward in a big way, starting a process that might result in fines totaling $3.3 million.

Facebook

The Hamburg Commissioner for Data Protection and Freedom of Information John Caspar has launched legal proceedings against the operator of the social network Facebook for illegally accessing and saving personal data of people who don’t use the respective social networking site.

Yahoo!

In 2009, following a cybercrime investigation by the Belgian police, it was discovered that a group was using Yahoo e-mail addresses to commit online fraud. The members of the group stole data from various companies and used the data to order goods without paying. Yahoo was requested by the Belgian Public Prosecutor to hand over the IDs related to the e-mail addresses used by the group but the company refused to comply and, on 2 March 2009, received a 55 000 euro fine from a Termonde judge who also imposed a daily penalty fee of 10 000 euro in case of non-compliance with the judgment. The court did not consider Yahoo’s argument that it was not subject to the Belgian law as it had no legal entity in Belgium and did not store any customer data in Belgium.

The Belgian Court of Appeal of Gand ruled on 30 June 2010 that Yahoo was not obliged to hand over personal data of its users to the Belgian authorities, in a case where the first instance had issued a contrary ruling.
U.K.

- (2010) From Tuesday 6 April, the Information Commissioner's Office (ICO) will get enhanced powers to fine organisations up to £500,000 for serious breaches of the Data Protection Act. Previously the maximum fine was a paltry £5,000. The most severe fines will be imposed in cases where the "data controller has seriously contravened the data protection principles and the contravention was of a kind likely to cause substantial damage or substantial distress.

- (2007) The Financial Services Authority (FSA) has fined The Nationwide Building Society £980,000 for the loss of a laptop which contained "confidential customer data" on 11 million customers.

- (2010) Zurich Insurance lost 46,000 customer records including some bank details when a tape back-up went missing between two sites in South Africa. Even worse, it took a year for Zurich UK to hear about the loss. Zurich Insurance must pay an enormous £2.3m fine for losing thousands of British people's personal data.

- (2009) The Financial Services Authority (FSA) has fined HSBC £3m for failing to properly look after its customers' information and private data. Also HSBC Life UK Limited (HSBC Life) was fined £1,610,000, HSBC Actuaries and Consultants Limited (HSBC Actuaries) was fined £875,000 and HSBC Insurance Brokers Limited (HSBC Insurance Brokers) was fined £700,000.

Spain

- (2009) On 24 September 2009, the Spanish Data Protection Agency imposed a EUR30,000 fine on Tick Tack Ticket, a leading live entertainment ticketing and marketing company, for sending commercial communications on the internet to 40,000 recipients without their consent. The sending of such unsolicited commercial communications took place in the context of a marketing campaign conducted by Tick Tack Ticket whereby participants were requested to provide the company with their friends' email addresses. Tick Tack Ticket thereafter used the email addresses that it gathered to send commercial communications without the recipients' express consent, which was in breach of Act 34/2002 on Information Society Services and E-Commerce.

Big Brother fine confirmed

- (2007) Spain's Supreme Court has confirmed the highest ever fine imposed by the country's Data Protection Agency. The 1,081,822 Euro fine was imposed against Zeppelin Television S.A. the producers of Spain's Big Brother television
programme for failing to protect the personal data of people applying to take part in the programme. The fine was originally imposed by the Spanish regulator in 2001.

The breaches of the DPA were that the company (i) did not comply with the information rights of the participants in the programme; (ii) did not obtaining their express consent for the processing of sensitive data; (iii) did not fulfil the requirements for data processing by third parties; and (iv) did not comply with regulations on security measures.

The facts that led to the investigation were that Zeppelin’s security system was breached and the data of the participants in the programme were made available over the internet.

### VI. Comparative table

<table>
<thead>
<tr>
<th>State</th>
<th>Max. fine (domestic currency)</th>
<th>Max. fine (in EUR)</th>
<th>GDP per capita (in PPS **) 2010 *)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>25 000 €</td>
<td>25 000</td>
<td>125</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>100 000 BGN</td>
<td>51 000</td>
<td>43</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>10 000 000 CZK</td>
<td>415 000</td>
<td>80</td>
</tr>
<tr>
<td>Denmark</td>
<td>/</td>
<td>/</td>
<td>125</td>
</tr>
<tr>
<td>Estonia</td>
<td>50 000 EEKroons</td>
<td>3 200</td>
<td>65</td>
</tr>
<tr>
<td>Finland</td>
<td>/</td>
<td>/</td>
<td>116</td>
</tr>
<tr>
<td>France</td>
<td>300 000 €</td>
<td>300 000</td>
<td>107</td>
</tr>
<tr>
<td>Hungary ***)</td>
<td>No sanctions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ireland</td>
<td>100 000 €</td>
<td>100 000</td>
<td>125</td>
</tr>
<tr>
<td>Slovak Republic</td>
<td>10 000 000 SKK</td>
<td>332 000</td>
<td>74</td>
</tr>
<tr>
<td>Slovenia</td>
<td>12 510 €</td>
<td>12 510</td>
<td>87</td>
</tr>
<tr>
<td>Spain</td>
<td>600 000 €</td>
<td>600 000</td>
<td>101</td>
</tr>
<tr>
<td>U.K.</td>
<td>500 000 £</td>
<td>570 000</td>
<td>114</td>
</tr>
<tr>
<td>Macedonia (FYROM)</td>
<td>2000 € (in DEN)</td>
<td>2 000</td>
<td>35</td>
</tr>
<tr>
<td>EU=27</td>
<td></td>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>

*) source Eurostat

**) Purchasing Power Standards (PPS)

***) A new Data Protection and Freedom of Information Bill - passed by the Hungarian Parliament (the Országgyűlés) in 2011 - will allow a newly formed Data Protection Authority (DPA) to impose fines between €380 - €37,000.
These indicators are not the measurement of effectiveness of sanctions. Effectiveness of sanctions depends not only of financial level but also on social, cultural, moral and other social aspects.

VII. Conclusions

The sanctions regime is an effective instrument for enforcement data protection legislation. As conclusion we may quote the idea of Mr Peter Hustinx, the EU Data Protection Supervisor, from his presentation in one conference in 2011: “Sanctioning violations of data protection law in the same manner as violations of competition law. The trade press regularly reports on multi-million euro fines for cartels or abuses of dominant positions by companies under the competition rules of the European Union. These figures are far away from the fines that currently can be levied for data protection violations. Observers of the competition law scene will agree that the main reason that companies operating in the EU pay attention to competition law is the astronomic fines that can - and are - levied”.

Observers of the privacy scene also agree that one of the reasons that privacy is sometimes still not taken as seriously as it should by companies, is the relative lack of enforcement, and the low fines in case of enforcement. With shrinking legal budgets for compliance and training, companies often devote more resources to areas where fines are steep such as competition law.

The European Union is reviewing the current 1995 Data Protection Directive and a draft proposal is expected this summer. Traditionally sanctions for violations of data protection laws have been left to the twenty-seven EU Member States (and they vary widely) but perhaps this will change. If accepted, it would revolutionize the data protection landscape in Europe. The Civil Liberties, Justice and Home Affairs Committee of the European Parliament adopted a report - on 15 June 2011 - which calls for the revised Directive 95/46/EC to include 'severe and dissuasive sanctions', including criminal penalties, for the misuse and abuse of personal data. The Committee said that "National data protection authorities should be given the necessary resources and be granted harmonised investigative and sanctioning powers". But we must wait for modernised text of Directive.

VIII. Recommendation

There are other forms of sanctions. The EU MS data protection legislation contents provisions of sanction in the form of financial penalty and liquidation
(erasure) of data collections. Other forms of sanctions are the matter of Criminal acts not data protection laws.

The effectiveness of sanctions shall evaluate under longitudinal observations by socio-economic criteria of the country. One of the criteria of effectiveness is influence to data controller to improve its wrong practice and avoid repetition of the breach of data protection legislation. The penalty as such, must send a clear signal to data controllers that the supervisory body (i.e. DPDP) intends to toughen controls over data processing activities taking place on the country. The beneficiary country range of fines (2000 € in MKD) seems ineffective. As example, this level of financial penalty may be enough for small companies or individuals for “minor infringement”. However, it is wanting for majority data controllers and breaches of LPDP. Such a range of fine doesn’t play the contribution role to improve quality processing and protection of personal data. It means that the DPDP has not effective tool for sanctioning serious and very serious breaches of the law by controllers of bigger institutions. From this view the DPDP is regarded as absolutely less powerful Data Protection Authority than is European average.