Data Protection Authority View on Data Breach Notification

Data Breach Notifications in Europe – The way forward. ENISA workshop

WOJCIECH WIEWIÓROWSKI PhD
Inspector General for Personal Data Protection, Poland

Brussels, January 24th , 2011

Generalny Inspektor
Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.giodo.gov.pl
kancelaria@giodo.gov.pl

CONTENT

- Legal basis of data protection in Poland
- Data Protection Authority in Poland
- Implementation of Telecom packet
- ”Enforcement”
- Sectoral or general

EUROPEAN DATA PROTECTION LAW

- Convention no. 108, Council of Europe
- Directive 95/46/EC
- Directive 2002/58/EC
- Charter of Fundamental Rights of the European Union (Article 8)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

POLISH DATA PROTECTION LEGISLATION

- The Act on Personal Data Protection – passed on 29 August 1997, entered into force on 30 April 1998
- Three law enforcement provisions (Regulations)

CONSTITUTION OF THE REPUBLIC OF POLAND (Art. 47)

Everyone shall have the right to legal protection of his private life and family life, of his honour and good reputation and to make decisions about his personal life.

CONSTITUTION OF THE REPUBLIC OF POLAND (Art. 51)

- No one may be obliged, except on the basis of statute, to disclose information concerning his person.
- Public authorities shall not acquire, collect or make accessible information on citizens other than that which is necessary in a democratic state ruled by law.
- Everyone shall have a right of access to official documents and data collections concerning him. Limitations upon such rights may be established by statute.
- Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute.
- Principles and procedures for collection of and access to information shall be specified by statute

POLISH DATA PROTECTION AUTHORITY (DUTIES)

- Supervision over personal data processing (both public and private sector)
- Issuing administrative decisions
- Considering complaints
- Keeping the register of data filing systems
- Issuing opinions on bills and regulations
- Activities to improve data protection
- International co-operation

From March 2011:

- Legislative inspiration
- Offical addresses
- Enforcement powers in administrative procedure

POLISH DATA PROTECTION AUTHORITY (DUTIES)

In case of any breach of the provisions on personal data protection, the Inspector General

shall order to restore the proper legal state, and in particular:

- to remedy the negligence,
- to complete, update, correct, disclose, or not to disclose personal data,
- to apply additional measures protecting the collected personal data,
- to suspend the flow of personal data to a third country,
- to safeguard the data or to transfer them to other subjects,
- to erase the personal data.

IMPLEMENTATION OF TELECOM DIRECTIVES

Art. 174a 1. In the case of a breach of personal data of subscriber or end user, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to Inspector General for Personal Data Protection.

The personal data breach shall mean security incident leading to accidental or unlawful destruction, loss, change, unathorised access to the personal data processed by telecom operatorin connection with ze publicly available electronic communications services.

2. In case he personal data breach may have adverse effects on personal data or privacy of a subscriber or end user, the provider of publicly available electronic communications services shall, without undue delay, notify the subscriber or end user.

IMPLEMENTATION OF TELECOM DIRECTIVES

Art. 174a

3. Notification mentioned in par. 2 shall not be required if the provider has demonstrated – according to the requirements of Inspector General for Personal Data Protection – that it has implemented appropriate technological protection measures which render the data unintelligible to any person who is not authorised to access it, and that those measures were applied to the data whose breach was notified.
4. if the provider has not already notified the subscriber or end user of the personal data breach, the Inspector General for Personal Data Protection, having considered the likely adverse effects of the breach, may oblige him to do so.
5. The notification concerned in par. 2 shall include:
   a) rescription of the nature of the personal data breach;
   b) telephone number, where more information on personal data breach can be obtained;
   c) recommendation on measures to mitigate the possible adverse effects of the personal data breach;
   d) information on the activities taken by the provider
6. The notification concerned in par. 1, apprt from data mentioned in par. 5 contains description of the measures proposed or taken by the provider to address the personal data breach.

IMPLEMENTATION OF TELECOM DIRECTIVES

Art. 174b. The Inspector General for Personal Data Protection may issue instructions for providers of publicly available electronic communications services concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made do guidelines issued by the European Commission.

Art. 174c. The provider of publicly available electronic communications services maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken according to Art. 174a par. 5 lit. d and par. 6.

Art. 174d. The Inspector General for Personal Data Protection may issue the guidelines to the providers concerning the best practices in personal data protection of subscribers and end users.

"ENFORCEMENT"

DPAs indicated that sanctioning authority enables them to better enforce regulations.
Data controllers will be less incentivised to comply with regulations if regulatory authorities do not have sufficient sanctioning powers. Some authorities indicated that financial penalties are seen as the most effective tool for pressuring data controllers to comply, while others indicated that public criticism and black lists could be effective too.

Sławomir Górniak (ed.) Andreas Rockelmann, Joshua Budd, Michael Vorisek Demosthenes Ikonomou, Rodica Tirtea: *Data breach notifications in the EU*, ENISA 2010, p. 5

SECTORAL OR GENERAL

So far such notification procedure is planned to be required only in Telecom sector.

Encourages *the Commission to explore the opportunity to extend data breach notification obligations to sectors other than the telecommunication sector. Data breach notification may, however, not become a routine alert of all sorts of security breaches. It shall only apply if the risks stemming from the breach can impact negatively the individuals' privacy and their personal data and the notification helps to protect the interests of individuals.*

Working materials of Article 29 WP

CONCLUSION

- Proactive approach ?
- Role of guidelines ?
- Legal status of guidelines ?
- Resources ?
- Sectoral ?
- Enforcement ?
- Harmonised approach ?
- International dimension ?

GIODO
Generalny Inspektor Ochrony Danych Osobowych

THANK YOU FOR YOUR ATTENTION !

desiwm@giodo.gov.pl
http://edugiodo.giodo.gov.pl