CASE TRANSLATION: LITHUANIA

Case citation / File number:
A-143-2740-12

Name and level of the court:
Lietuvos vyriausiasis administracinis teismas (Supreme Administrative Court of Lithuania)

Date of decision:
18 December 2012

Electronic signatures; qualified certificate; advanced electronic signature; personal identification numbers; data protection

Title: Case [A-143-2740-12] Doc

File No: A-143-2740-12

File type: administrative proceedings

Court: Higher Administrative Court of Lithuania

Parties:

Applicant

State Enterprise Center of Registers

Defendant

State Data Protection Inspectorate

Interested third parties

Population Register Service under the Lithuanian Ministry of the Interior

Information Society Development Committee under the Ministry of Transport

Communications Regulatory Authority

Private Company Digital Certification Centre

DECISION

of the

HIGHER ADMINISTRATIVE COURT OF LITHUANIA

of 18 December 2012

Vilnius

Lithuanian Higher Administrative Court composed of judges Laima Baltrūnaitė (Chairman), Anatolijus Baranovas (Rapporteur) and Irmantas Jarukaitis,

secretary Lilija Andrijauskaitė,

in the presence of applicant's representative Jurgita Apanskiene,

defendant's representative Simona Gavorskaitė,

the interested third party, Lithuanian Communications Regulatory Authority, representative Marina Lavrinavičiūtė,

the interested third party, Private Company Digital Certification Centre, representative Mudrik Dadašov,

in the administrative proceedings started by the applicant, State Enterprise Centre of Registers, against the defendant State Data Protection Inspectorate, the interested third parties, the Lithuanian Communications Regulatory Authority, the Information Society Development Committee under the Ministry of Communications, Office of the Register of Population of the Republic of Lithuania under the Ministry of Internal Affairs, Private Company Digital Certification Centre for the annulment of the defendant's Order,

whereas the appeal proceedings have been started by the defendant, the State Data Protection Inspectorate, seeking to have set aside the decision of Vilnius District Administrative Court of 11 April 2012 ('the contested decision'),

decides as follows,

Decision

Background to the dispute

I.

The applicant, the State Enterprise Centre of Registers ('the applicant') brought a complaint to the Vilnius District Administrative Court (Court of first instance) for annulment of the order 'On the processing of personal data' No. 2R-3659 (2.13) dated 14 November 2011 ('Order') issued by the defendant, the State Data Protection Inspectorate ('the defendant' or 'the appellant').

The applicant requested an annulment of the Order since it does not meet the statutory requirements and therefore is not justified. The applicant noted that the State Enterprise Center of Registers, in accordance with its legal nature and the functions, is a public administration body. The issuance of qualified certificates should be regarded as a public administration activity, because, according to Law on Electronic Signature, the main purpose of issuing such certificates is to create qualified electronic signatures, proving a person's identity in cyberspace. The principles of issuing qualified certificates have been set out in the Resolution of the Government of Lithuania No. 2108 of 31 December 2002 on the requirements to service providers issuing qualified certificates, and the requirements for devices of electronic signature and the registration of such service providers and the electronic signature supervision scheme ('Resolution No. 2108'). According to the Clause 5 of the Resolution No. 2108, service providers must validate their Certificate Practice Statements ('CPS') and publish them on-line. According to Resolution No. 2108, the supervision of service providers issuing qualified certificates has been conducted by the Information Society Development Committee under the Ministry of Transport ('Committee') until 19th of January 2011, and from 20th of January 2011 this supervision is performed by the Lithuanian Communications Regulatory Authority ('Communications Authority').

The CPS (the first edition) of the applicant was published on its web site in September 2008, after it had been approved by the supervisory body – the Committee. Therefore Order No. V-226 adopted by the State Enterprise Centre of Registers on 24 November 2010 has to be considered as a normative administrative act, the provision of which (putting a personal code into the qualified certificate) must not be recognized as contradicting the provisions of the Law on Legal Protection of Personal Data or any other requirements/orders of the abovementioned state administration institutions.

In addition, as has been ruled in the judgment of the Higher Administrative Court of Lithuania on 29 August 2011, in case No 575-392/2011, the abovementioned administrative act has only validated other acts (Certificate Policy and Certificate Practice Statement). This means that the act has enforced the functions of the applicant regarding the Law on Electronic Signature.

While establishing the content, structure and procedures of qualified certificates, the State Enterprise Centre of Registers followed the rules of the Law on Legal Protection of Personal Data that were valid on 12 February 2003 (in force on 1 July 2003). According to article 7(3) of the mentioned law, the personal identification number can be used in the public records and information systems without the consent of the data subject, if allowed by legal acts.

However, despite the abovementioned provisions of the law that permits the State Enterprise Centre of Registers, as a qualified certificate provider, to use the personal identification number without the data subject's consent, the State Enterprise Centre of Registers in all cases informed and signed the contracts with its customers regarding the use of personal identification numbers in qualified certificates.

When creating qualified certificates, it is necessary to follow the provisions of the Law on Legal Protection of Personal Data and provisions of other mandatory legislative acts. Pursuant to article 2(5) of the Law on Electronic Signature the safe electronic signature is defined as the one that meets all the requirements specified: 1) it is uniquely linked to the signatory; 2) allows the identification of the signatory; 3) is created by tools that the signatory can control by his request; 4) is connected with the personal data in a way that all the changes are detectable. In addition, pursuant to article 2(15) of the Law on Electronic Signature, specific attributes can be inserted in the qualified certificate if such information is necessary. The applicant emphasized that according to the current legislation there is no other special attribute, other than personal identification number, that would allow the individual to be unambiguously identified. Qualified certificates can be used to obtain access to the on-line services of the public institutions, therefore the personal identification number, being the unique identifier, is mandatory in qualified certificates.

Lithuanian legislation provides that a person can be identified by name, address and personal identification number, however a person cannot be identified simply by name and surname, as there can be several individuals with same names and surnames. Therefore, the personal identification number is the only data item that is not misleading, and when used in a qualified certificate, in its essence has to be considered equal to an ID or passport. Among other things, the applicant pointed out that article 7 of the current Law on Legal Protection of Personal Data does not prohibit the use of a personal code in the State registries and information systems if they are allowed by legal acts. The law explicitly prohibits making the personal identification number publicly available, and prevents the collection and use of the personal identification number for direct marketing purposes. The applicant argues that issue of qualified certificates for signing e-documents and e-mails does not make these certificates, nor the personal identification numbers public. The certificate holder chooses for which purpose he/she wants to use the qualified certificate.

Defendant asked to dismiss the complaint as unfounded.

The defendant stated that according to the applicant's procedures, the use of the personal identification number in the qualified certificates should not be regarded as the use of a personal identification number in State registries and information systems, when such data is made available to the receiver of the electronically signed document.

The use of a personal code for signing e-documents and e-mails cannot be considered as conforming with the criteria of lawful processing of personal identification number as set out in article 7(2) of Law on Legal Protection of Personal Data. The law establishes the necessary requirement of obtaining the data subject's consent. The data subject should be able to choose whether or not to use the personal code for signing e-documents and e-mails. The refusal to use the personal identification number would result in an inability to use the applicant's service – to sign with an electronic signature. On the other hand, the person who received a signed e-document or e-mail cannot use the personal identification number in the certificate to verify the identity of the signatory, because the recipient has no prior knowledge of the personal code of the signatory. Furthermore, no personal identification number is required when signing the paper documents.

Since the validity of the electronic signature is determined after the status of the certificate is primarily confirmed by the certification service provider, there is no need to use the personal identification number to verify the identity of the signatory. The defendant pointed out that according to the Order, the use of a personal code for signing e-documents and e-mails is excessive management of personal data (personal identification number). By issuing a certificate with a personal identification number, the applicant breaches the article 3(1), point 4 of the Law on Legal Protection of Personal Data. The use of a personal identification number in the electronic signature creates a possibility for uncontrolled distribution of the signatory's personal identification number.

The rapid increase of use of electronic signatures means that the personal identification number may be disclosed to an unlimited number of third parties and used without control. The personal identification number would be disclosed to the receiver of signed e-document or e-mail, it also could be stored in the recipient's computer. Moreover, the holder of e-signature would be obliged to disclose his/her personal code when signing other e-documents (e.g., on the Internet), petitions or similar instruments.

According to the article 3(3) of the Law on Electronic Signature, the verification of the signature is public, whereas article 7(4) of the Law on Legal Protection of Personal Data prohibits making the personal code public. In addition, according to article 8(3) and article 4(9) of Law on residents' register, the personal identification number is a unique and unalterable identifier used for collecting individual data. If the personal identification number is widely available, the increase of the possibility of unauthorized access in the state registers and information systems might cause the violation of a person's privacy. There is a risk that the personal identification number might be made available and used without a legitimate purpose. It would lead to violation of articles 3 and 7 of the Law on Legal Protection of Personal Data.

Furthermore, article 8(1) of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures obliges Member States to ensure that the certification service providers and other national authorities responsible for the accreditation and supervision of these providers comply with the requirements of Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Accordingly, the development of the information society and the implementation of electronic signatures must be exercised in accordance with the data protection requirements.

The interested third party, the Communications Authority, pointed out in its explanations that in accordance with article 4(9) of the Law on residents' register, the personal identification number is a unique sequence of eleven digits that identifies a person, enables the collection of data about a person, and ensures the interoperability of the state registers and information systems. These provisions lead to the conclusion that a personal identification number is one of the items of primary personal data enabling the identification of a person. Also noted that according to article 2(14) of the Law on Electronic Signature the certificate is defined as an 'electronic attestation which links signature-verification data to the signatory', and 'approves or allows the identification of the signatory'. According to article 2(15) of the same law, a qualified certificate is a certificate 'issued by the government's service provider or its authorized authority which complies with the certification requirements'.

Before issuing a qualified certificate, the certification service provider takes the following steps in order to identify the person: carries out an identity check and requests a proof of valid identity documents with the personal identification number (paragraph 8, 9 of the Schedule on the issue of certificates and consultation procedures approved by the Order of the Director of Electronic Communications No. 1V-406 of 19 April, 2011 ('Schedule')); collects and stores all the information and documents obtained (paragraph 10 of the Schedule); provides a certificate number in the qualified certificate and keeps a record of it (article 2(15) point 7 of Law on Electronic Signature). It is therefore concluded that the signatory's identity is determined according to his/her identity document that is provided for receiving a qualified certificate. Furthermore, it is noted that the personal identification number is not obligatory in the qualified certificate according to the Law on Electronic Signature. However, the law provides that the certification service provider can include other special attributes of the signatory if it is necessary for the adequate use of the qualified certificate. According to the Communications Authority, if this is the question, the personal identification number can be regarded as a special attribute in a qualified certificate.

The interested third party the Committee agreed with the complaint.

The Committee pointed out that in some cases, the electronic signature has to confirm the data and identify the signatory. In fact, the electronic signature certificate serves to identify the person. An electronic signature must not only identify the signatory, but also confirm his/her identity. It is noted that the list of documents proving personal identity can be found in the Passport Law. Such documents are the passport – confirming the Republic of Lithuania citizen's identity, and the identity card – confirming person's identity and citizenship. Both the passport and identity card must provide a personal identification number. The Lithuanian passport or identity card and a certificate in cyberspace can be considered to some extent as equivalent documents, because, although they are not identical in the terms of the use, they perform the same function – identifies the person. The personal identification number comprises the basic personal data and enables a person to be identified. Otherwise, a person's identity could be determined only by using other types of personal data (name, address, residence address, date of birth and so on). The personal identification number is the main type of personal data, which allows for the direct identification of the person. According to article 2(15) point 4 of the Law on Electronic Signature, specific attributes can be written in a qualified certificate if it is necessary for its use. Therefore, the Committee believes that the law does not prohibit the use of a personal identification number in the certificate. It is emphasized that often the signatory's name and personal identification number is indicated in paper documents (applications, contracts and so on) if other personal information is unknown. By signing documents in cyberspace with an electronic signature, the personal identification number enables a person to be automatically and unambiguously ascertained. The Committee recognized that the signatory must be given an opportunity in some cases (for example, signing public documents) not to disclose a personal code, in order to protect his/her legitimate interests. Until 1 May 2011, the Committee implemented the power attributed to it as a supervision authority of electronic signatures that included the registration of certification service providers. According to paragraph 9 of the Government's Resolution No. 2108 of the 31 December 2002 on the registration procedures of certification service providers ('Registration procedure'), the Committee had a duty not to register the certification service provider if the documents provided did not meet the established requirements or an application and other documents contained incomplete or incorrect data. These requirements are set up in the abovementioned resolution, which includes the requirements for the service provider's internal administration system, service activities, and etc.

The interested third party, the Population Register Service under the Lithuanian Ministry of the Interior ('Population Service') asked to resolve the case in court's discretion.

The Population Service stated that currently a personal identification number is recorded in qualified certificates of the identity cards. During preparation for the practical implementation it was found that refusing to provide a personal identification number in the certificate would lead to identification problem. In practice, it may occur that two people have the same names and the same date of birth, therefore only different codes then can distinguish persons. Signing paper documents, identification number is not required, but in practice (e.g., signing insurance, utility service, telecommunications service and other agreements) it is always asked with identification document. Such information is always checked. In cyberspace, the contract party needs to make sure that the signatory is the one who has the right to sign the document. The identification of the signatory is also important for e-banking, especially for electronic bank transaction. The beneficiary (the bank) of signed electronic document must ensure that the signatory is really the person who has the right to manage a bank account.

The interested third party, the 'Digital Certification Centre', requested the court to dismiss the complaint as unfounded.

The 'Digital Certification Centre' indicated that Law on Legal Protection of Personal Data prohibits the publication of a personal identification number, and that it is an obligatory provision. Even if article 2(15) point 4 of the Law on Electronic Signature provides that the special attributes can be used in the certificate, if it is necessary for the purposes for which the certificate is going to be used, it cannot overrule the general provision of the Law on Legal Protection of Personal Data. According to the law, it is prohibited to make the personal identification number public. Any additional personal attributes that are not directly provided by the legislator can be added to a qualified certificate if the certification service provider ensured that such attributes or methods of use confirms with the European Union and the Lithuanian law; is related with potential hazards or risks to the holder of the certificate, and the user of the certificate is warned in advance, indicating the specific risks (e.g., possible uncontrolled dissemination of personal data); the qualified certificate contains the link to the public information about the certification service provider with a clear and detailed statement of the purposes of the use of a qualified certificate (as required by the Law on Electronic Signature). It was argued that article 7(1) of the Law on Legal Protection of Personal Data provides that the personal identification number is a unique sequence of numbers. The personal code is issued in accordance with Law on Residents' register. Among other things, it was pointed out that the State Enterprise Centre of Registers is electronic services provider. At the same time, it provides commercial services which are not provided for by the law. The service of issuing qualified certificates is a commercial service of this public body. The State Control of the Republic of Lithuania expressed its views on the controversial commercial certification activities of the applicant. Each qualified certification service provider must be registered within the Lithuanian electronic signature supervisory institution. The 'Digital Certification Centre' was the first qualified certification service provider legally registered in 2005. During the initial activity of registration, the company received a note from the inspectorate about the use of the personal identification number in a qualified certificate. In order to meet the requirement of state authorities, the 'Digital Certification Centre' removed the personal identification number from the certificates. The 'Digital Certification Centre' was then officially registered as a qualified certification service provider. The applicant registered their commercial electronic certification activities with the supervisory institution in 2008. In accordance with the general procedure at the time of the registration, the applicant knew the requirement for the use of the personal identification number. However, despite the fact that the applicant's services did not fulfil the legal requirements, its commercial activities were registered that led to two different precedents in the registration procedures in Lithuania. Two economic entities became operational in the market: 'Digital Certification Centre', which satisfied the obligatory requirements, and State Enterprise Centre of Registers, apparently ignoring these requirements.

Performing public and commercial services at the same time, the applicant *de facto* inserts into its public services qualified certificates that contain a personal identification number. So, in a short period of time the applicant has acquired a dominant position in the market of digital certificates. Holding a monopoly right in the field of public electronic services and wishing to reinforce the dominant position in the market, the applicant started to demand qualified certificates with the personal identification number. This is the second precedent when due to the legal nihilism of the State Enterprise Centre of Registers, 'Digital Certification Centre' has suffered direct damages. The applicant in the current procedures attempts to legitimize its questionable *status quo* and avoid responsibility for the illegal issue of thousands of qualified certificates with individual identification number, as well as prevent responsibility of the use of the European Union structural funds for the development of public electronic services.

The decision of the court of first instance

II

In the contested decision, Vilnius District Administrative Court found the appeal admissible and well founded. The court of first instance annulled the Order of the defendant.

The court found that a matter of dispute in the case in question is the legitimacy and validity of the Order, and the object of the dispute – the use of personal identification number in a qualified certificate. The court followed the provisions of articles 5(1), 22(1) and 3(2) of the Law on Administrative Proceedings. The court evaluated the written evidence. It also followed article 4(9) of the Law on Residents' register, articles 1(1), 2(1) and 2(4), 3(1) part 4, of the Law on Legal Protection of Personal Data, articles 2(4), 2(14), 2(15) of the Law on Electronic Signature, paragraphs 8, 9, 10 of the Schedule, and article 1 (1) point 2 of the Identity Card Act. Systematic analysis of legal norms presupposed the conclusion that a personal identification number can be used in the certificate for the purpose to authenticate and identify the signatory. The signatory's identity is determined from his personal identity documents that must be provided before issuing a qualified certificate. Although article 2 (15) of the Law on Electronic Signature does not require the inclusion of the personal code in an electronic certificate, the law gives the right to a certification service provider to add specific attributes of the signatory if it is necessary in the view of the use of the certificate. The court considered that the personal identification number can be regarded as a specific attribute. Moreover, articles 57 and 86 (2) of the Law on Administrative Proceedings were followed. The court ruled that the proper assessment of the facts and application of the law are closely linked. Only the establishment of relevant facts, necessary for the proper application of the law, and the legitimate and justified decision can be made. Taking into account the written evidence, relevant legislation, principles of justice and reasonableness, the well-established case law (case of the Administrative Supreme Court of Lithuania No. 575-392/2011 of 29 August 2011), the court ruled that legislature does not forbid the defendant to use a personal identification number with the person's consent (usually a person signs the agreement regarding the use of the personal code). The court found that the Order is illegal and unjustified. The defendant incorrectly interpreted and applied the substantive law and has issued the illegal Order that is contrary to the primary legislation. The Order therefore has been annulled.

Grounds of appeal

III

In the appeal, the appellant seeks to have set aside the contested decision. The appeal is based on the following grounds:

1. The appellant does not contest the legality of verifying a person's identity prior to the issue of a qualified certificate nor the use and storage of personal data by the certificate provider. However, the appellant claims the use of the personal identification number in a qualified certificate for signing of e-documents and e-mails.

2. The Identity Card Act does not regulate the qualified certificates issued by the State Enterprise Centre of Registers. According to article 3.3.1(d) of the States Enterprise Center of Registers' rules of 24 November 2010, approved by State Enterprise Centre of Register Director, qualification authorities shall require that the issued certificate will at least indicate the following data: name(s) and surname, personal code.

3. Neither the Law on Electronic Signature, nor any other law regulating activities of the State Enterprise Centre of Registers, clearly and unequivocally require the use of the personal identification number in a

qualified certificate. Therefore, differently from the person's name and surname, it cannot be considered that the use of the personal code in the qualified certificates complies with the legal criteria established in article 7(3) point 1 of the Law on Legal Protection of Personal Data.

4. A person cannot choose to use or not to use the personal identification number in e-documents and e-mails. If a person refuses to use such data, he/she does not receive the requested services from the applicant (a qualified digital electronic signature certificate is not issued). Therefore it cannot be held that the use of the personal code when signing electronic documents complies with article 7(2) of the Law on Legal Protection of Personal Data, where the prerequisite for lawful use is consent from the data holder. The use of the personal identification number in electronic signatures shall be regarded as excessive. The State Enterprise Centre of Registers infringed article 3(1) point 4 of the Law on Legal Protection of Personal Data by using the personal identification number as an excessive amount of data in a qualified certificate.

The respondent asks the court to uphold the contested decision and dismiss the appellant's appeal as unfounded. The respondent puts forward the following grounds in its response:

1. The law does not prohibit the use of the personal identification number for authentication purposes and for the identification of person in the qualified certificate. Furthermore the personal identification number can be treated as a special attribute within the meaning of article 2(15) point 4 of the Law on Electronic Signature, when it is necessary for the use of a qualified certificate.

2. All certification service providers who are empowered to issue the digital identification documents must apply legal acts, regulating personal identification questions in cyberspace, equally – the Law on Electronic Signature and the Law on Legal Protection of Personal Data and the Identity Card Act.

3. It is important to understand and correctly evaluate the importance of a qualified certificate and its validity. The law distinguishes an electronic signature and an advanced electronic signature. When issuing an advanced electronic signature, the inclusion of a personal code in the qualified certificate is not only possible, but necessary. A personal code is the only and unique characteristic of a person in the country. The requirement not to use the personal identification number in the qualified certificate is unfounded.

4. When a qualified certificate is issued, the person is informed that the code is indicated in the documents. A qualified certificate is issued only with the written person's consent (when signing an agreement). The state body has no right to prohibit a holder of a qualified certificate to use his personal identification number. Qualified certificates are issued for the use and creation of a secure electronic signature.

The third interested party, the Communications Authority, states that it upholds its previous position set out in the explanatory notes in the court of first instance. It is indicated that the use of a personal identification number in a qualified certificate is not prohibited to authenticate the data and verify the identity of the signatory. It may be regarded as a specific attribute within the meaning of article 2(15) point 4 of the Law on Electronic Signature, if it is necessary for the use of the certificate.

The third interested party, the Committee, asks the court to uphold the contested decision.

The Committee repeats previously stated arguments, indicating that it does not consider that the use of the personal code in the electronic signature certificate is superfluous. The evaluation of the legality of use shall be determined taking into account the purposes for which the certificate is used. A personal identification number is made public by a signatory of the electronic document, and not by the certification service provider. A person himself chooses the certification services provider and is not forced to choose the certification service provider that necessarily uses a personal code in the electronic signature certificate. However, the signatory must be given an opportunity in some cases (for example, when signing public documents) not to disclose a personal identification number, in order to protect the legitimate interests of processing personal data.

The third interested party, the Population Register Service, in the response to the appeal, repeats the previously made arguments, and requests the court to rely on the provisions of the legislation and principles of reasonableness and justice and solve the case in court's discretion.

The fourth interested party, 'Digital Certification Centre', asks to set aside the contested decision of Vilnius District Administrative Court and issue a new decision. It submits the following arguments:

1. The systematic analysis of the circumstances of the use of the qualified certificate shows that the Law on Electronic Signature *de facto* prohibits the use of a personal code in the qualified certificate. The court wrongly compared the certificate with an identity document. The applicant limits the choice of the consumers, violates the law protecting of personal data and restricts the possibility of the consumers to control the use of their personal identification number when the electronic signature document is transferred to another parties.

2. According to article 15(2) of the Law on Electronic Signature, a qualified certificate can be supplemented with the individual's attributes (but not identifiers), when it is needed for the use of the certificate. However, there is no legal ground to add any identification details in the certificate. Therefore, the contested decision created preconditions for the unauthorized use of the personal identification number in qualified certificates.

Findings of the Higher Administrative Court of Lithuania

IV

The appeal is upheld.

The essence of this administrative dispute is the applicant's right to include a personal identification number in the qualified certificates according to the Law on Electronic Signature. From the facts of the case it is seen that the appellant bases such a right from the definition of 'qualified certificate' as it is given in article 2(15) of the Law on Electronic Signature. According to the mentioned law (article 2(15) point 4) a qualified certificate, among other things, can include 'the special attributes of the signatory, if it is necessary for the purposes for which the certificate is going to be used'. According to the appellant, the personal identification number can be regarded as a special attribute, therefore it can be legally included (indicated) in the qualified certificate.

The appellant bases its position on the provisions of the Law on Legal Protection of Personal Data, where it is set that the data controller (in this case, the appellant) is responsible for ensuring that the personal data is used 'only as much as it is needed for the collection and processing of data' (article 3(1) p. 4), and restrictions on the use of personal identification number are imposed (article 7(2), p. 4).

Firstly, taking into account the positions of the parties, the interdependence of the abovementioned laws must be determined and must be established which of them is the special law, having the priority in the case under appeal. With regard to the facts of the case, it should be noted that the parties do not argue about the disclosure of the personal data (the electronic signature of the holder and the personal identification number) in the qualified certificate to the direct addressee (recipient) or other third party, when electronic documents or e-mails with digital signature are submitted or transmitted to other party.

Regarding the interaction between the Law on Electronic Signature and the Law on Legal Protection of Personal Data, it is noted that the objects regulated by the Law on Electronic Signature are the electronic signature (secure electronic signature), the certificate (a qualified certificate) and the link between a signatory and the signed data. These objects, by their nature, are attributable to personal data, regulated by the Law on Legal Protection of Personal Data (such conclusion can be made from the legal descriptions of the terms). Therefore, it must be concluded that the Law on the Legal Protection of Personal data is a special law and has superiority over the Law on Electronic Signature. Furthermore, article 12(1) point 3 of the Law on Electronic Signature obliges the certification service provider (in this case the applicant) to ensure the protection of personal data when issuing the certificate, as it is provided in the Law on Legal Protection of Personal Data and other legal acts of the Republic of Lithuania. This means that the provisions of the Law on Legal Protection of Personal Data, regulating the processing of personal data and setting the prohibitions and restrictions for such data, directly and without any reservation applies in the legal field regulated by the Law on Electronic Signature, especially where it concerns the management of personal data, the creation and the issuance of the qualified certificates and personal signatures. Subject to the foregoing arguments, it is concluded that article 2(15) point 4 of the Law on Electronic Signature can be applied in the present situations as far as it does not conflict and is in accordance with the Law on Legal Protection of Personal Data.

It is noted that the data controller's (the applicant can be regarded as a data controller according to article 2(7) of the Law on Legal Protection of Personal Data) obligations in processing personal data are set out in article 3 of the Law on Legal Protection of Personal

Data (relevant edition No.XI-1372 of 5 December 2011). The article indicates that the data controller must ensure that personal data is adequate, relevant and does not go beyond what is necessary to collect and process such data. The mentioned article provides the criteria according to which the scope of personal data must be determined, and that it is closely related with the collection and the further handling of such data. The different criterion must be established in each case depending on the assessment of a certain situations. The evaluation of each situation allows the determination of the minimum scope of the personal data that needs to be collected by the controller in order to perform its operations and handle the data further according to the legislative requirements. In other words, if the data controller (the appellant) can objectively perform its functions (in this case functions set out in the Law on Electronic Signature) without the disputed personal identification number, such data according to article 3(1) point 4 of the Law on Legal Protection of Personal Data shall be deemed excessive and such use prohibited.

It is clear from the facts of this case, that the personal identification number (the requirement for a person to submit the personal identification number) is needed for the applicant before forming the certificate (the qualified certificate) to determine (check) the identity of the person, i.e. before issuing the certificate and processing the data. Otherwise, the applicant would not be able to ensure the unambiguous identification of the electronic signature holder. It should be noted that a use of a personal code in such situations is established under paragraph 8 and 9 of the Schedule, and that the defendant does not object such use. However, comparing the use of a personal code in a qualified certificate with the ability of the applicant to carry out the management functions of these certificates, it is noted that the absence of a personal identification number in the qualified certificate does not preclude the appellant, as a certification service provider, to carry out his duties. Such conclusion, among other things, is confirmed by the third party concerned 'Digital Certification Centre' that performs the same duties. Given the above considerations, it follows that the appellant's use of the personal code in a qualified certificate according to article 3(1) point 4 on the Law on Legal Protection of Personal Data is illegitimate.

Taking into account the specific issue of the personal identification number and that this number has a unique significance in the field of human rights, article 7 on the Law on Legal Protection of Personal Data sets out special rules for its use. This means that a special condition for the use of the personal identification number, as established in the legislation, is applicable without exception to all situations. The restrictions and prohibitions to use personal code are provided in article 7(2) of the abovementioned legislation (version No. X-1444 of 2 January 2008). This article states that the management of the personal identification number can be done only with the data subject's consent, except in situations when the use of personal identification number is prohibited (article 7(2) points 4 and 5). The law prohibits making the personal code available to the public. When applying specified provisions of article 7 in the present situation, it is noted that data subject's consent to use his personal code, as mentioned in second part of the article, would imply a situation where the data subject clearly and unambiguously understands the use of his/her personal data, the necessity to make such use and has an interest in such use. (In this context, it should be noted that this situation corresponds to the abovementioned use of the personal identification number when determining the identity of the signatory prior the issues of qualified certificate, i.e. prior the management of certificate and the personal data). On the contrary, in a situation where the data subject does not know and cannot know the circumstances of the use (disclosure) of the personal identification number (the situation when digitally signed document is transferred to other persons), the condition of article 7(2) of the Law on Legal Protection of Personal Data – the consent given from the data subject – is not met.

Article 7(4) of the Law on Legal Protection of Personal Data imperatively prohibits to publish (make public) the personal identification number. This rule shall be interpreted by the linguistic method. According to the Lithuanian dictionary, one of the meanings of the word 'public' is open, non-confidential. The meaning of the word 'publish' – the dissemination of knowledge ('Modern Lithuanian Dictionary', Lithuanian Language Institute, Vilnius, 2000, page 931, 701). The above-discussed situation when the personal identification number is disclosed and transferred to an indeterminate number of persons together with the digital signature, is understood as one of the ways of making 'publicly available'. This allows the court to conclude that article 7(4) of the Law on Legal Protection of Personal Data is infringed in the present case.

Taking into account the findings of the court, it follows from all of the above considerations that the appellant's complaint cannot be upheld and must be rejected. The Court of First Instance incorrectly interpreted and applied the substantive law relevant in this case. Therefore, the contested decision is annulled (according to article 143 of the Law on Administrative Proceedings).

Order

In accordance with the article 88(1), article 136, article 140(1) point 2 of the Law on Administrative Proceedings,

The Court hereby:

Annuls the Vilnius District Administrative Court decision of 11 April 2012 and dismisses the appellant's, the State Enterprise Centre of Registers, complaint as unfounded.

The decision is final.

Judges

Laimė Baltrūnaitė

Anatolijus Baranovas

Irmantas Jarukaitis

With thanks to **Jurate Breimelyte** for her help with this translation.

COMMENTARY:

Data protection law and personal identification numbers in Lithuania

By **Mindaugas Kiškis**

Lithuania has been a member of the European Union since 1 May 2004, and diligently follows the EU guidance on regulating personal data protection. Data protection has been comprehensively regulated in Lithuania since 1996 by the special Law on Legal Protection of Personal Data (the current legislation in force is Law of 23 February 2008 (effective from 1 January 2009) with subsequent amendments effective from 1 September 2011) (Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas 1996 m. birželio 11 d. Nr. I-1374).

The Law on Legal Protection of Personal Data implements the EU Data Protection Directive 95/46/EC,[1] and also provides specific national rules on many additional issues of national importance, such as the processing of personal identification numbers. Other areas of specific national data protection regulation include, but is not limited to regulations on data protection in the healthcare and medical fields, regulations on public polls, direct marketing, management of debtor information, credit bureaus and credit referencing and video surveillance.

Generally, the Lithuanian government officials and judges have adopted strict approach to the interpretation of the Law on Legal Protection of Personal Data. Normally, the data subject is given the benefit of the doubt and the legal regime tends to be restrictive of personal data processing. The definition of personal data in the Law on Legal Protection of Personal Data is based on the standard definition of personal data found in the EU Data Protection Directive 95/46/EC. It applies to any data pertaining to an identifiable individual. Case law and administrative practice interprets the definition increasingly broadly. Information is treated as personal data if publicly available material can be used to indirectly identify the relevant individual. In particular, IP addresses, car license plates and postal addresses (excluding the name) have been recognized as personal data.[2]

On the other hand, infringements of the data protection regime are subject to insignificant financial sanctions (up to 600 euro), and overall the enforcement (especially against public data controllers) leaves a lot of room for improvement. The State Data Protection Inspectorate is the authorized data protection authority and supervisor of the Law on Legal Protection of Personal Data. In its activities it most often relies on issuing administrative orders demanding discontinuation of infringing data processing, but is short on strong enforcement powers.

Personal identification numbers in Lithuania were introduced in the early 1990s. The personal identification number is composed of 11 digits, is uniquely attributed to each individual and is printed in his passport and personal identity card. Unfortunately, at the time when personal identification numbers were introduced in Lithuania, the privacy considerations were not ascertained and the data protection regulations were not in place. Because of this, the structure that was chosen for the personal identification number in Lithuania was not random. Instead, it directly provides information about the sex (1 number out of 11) and the date of birth (6 numbers out of 11) of the individual. Only the last 4 digits in the Lithuanian personal identification number are random and independent from the other information about the individual. Thus, the Lithuanian personal identification numbers by themselves are carriers of extended private information, which generally are additional to the personal identification number.

This design flaw was recognized by the mid 1990s when the Law on Legal Protection of Personal Data was introduced, but by that time the practical and cost considerations prevented the change of the

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 P. 0031 – 0050.

[2] See for example 26 July 2012 ruling of the Higher Administrative Court of the Republic of Lithuania in case No. A858-2133/2012 on car license plates and the broad interpretation of ‘personal data’.

system – all of Lithuania’s population was issued with a personal identification number and public information registers were designed around them.

In an attempt to rectify the privacy flaws of the personal identification number, the special legal rules for the processing of personal identification numbers were included into the Law on Legal Protection of Personal Data. Article 7 of the Law on Legal Protection of Personal Data sets forth an augmented legal protection regime for the personal identification numbers. Principal rules are akin to the rules applicable to sensitive personal data and are described below.

The use of the personal identification number is permitted when processing personal data only with the consent of the data subject. According to paragraph 3 of article 7 of the Law on Legal Protection of Personal Data, personal identification numbers may be used without the consent of the data subject only if:

(i) such a right is laid down in the law; or

(ii) it is processed in state or institutional registers and information systems, provided that they have been officially set up according to the law; or

(iii) it is processed by legal persons involved in activities relating to the granting of loans and recovery of debts, insurance or financial leasing, health care and social insurance as well as in the activities of other institutions providing and administrating social care, educational establishments, science and studies institutions; or

(iv) it is processed for the purpose of classified data in cases laid down by legislation.

Pursuant to paragraphs 4 and 5 of article 7 of the Law on Legal Protection of Personal Data, the personal identification number may not be made public, and personal identification numbers may not be collected and processed for direct marketing purposes. Legal persons, who process personal identification numbers for legitimate purposes, may use the personal identification number only for the purpose for which it has been received and only in cases where it is necessary for a legitimate and specified purpose of personal data processing.

Due to the strict personal identification number processing criteria, it became a routine inquiry for the State Data Protection Inspectorate of the Republic of Lithuania to check and evaluate processing of personal identification numbers.

Background of the case

Against the background noted above, the State Enterprise Centre of Registers (the plaintiff in administrative case No. A-143-2740-12), who is the data controller for the principal state or institutional registers and information systems in the Republic of Lithuania, interpreted the personal identification number processing rules as allowing them to process the personal identification number for the purposes of qualified electronic signatures. To be precise, the personal identification number was technologically incorporated into the public qualified electronic signature certificates (as part of the data comprising the qualified certificate) issued by the State Enterprise Centre of Registers.

The State Enterprise Centre of Registers justified such use of the personal identification number by the official status and public powers granted to the State Enterprise Centre of Registers in legislation, as well as by the rules on the qualified electronic signature certificates provided for in the Law on Electronic Signature (Lietuvos Respublikos elektroninio parašo įstatymas 2000 m. liepos 11 d. Nr. VII-1822). According to such rules, the qualified certificate ‘may include special attributes of the signatory, if this is necessary for the purposes for which the certificate is going to be used’.

The State Data Protection Inspectorate (the defendant in administrative case No. A-143-2740-12) held that the use of the personal identification numbers in the public qualified electronic signature certificates was not justifiable under the special rules of the Law on Legal Protection of Personal Data, as well as being excessive under the general principle of using only a minimum of personal data required for the purpose. Therefore, the State Data Protection Inspectorate issued an administrative order to the State Enterprise Centre of Registers, demanding a discontinuation of the use of the personal identification numbers in public qualified electronic signature certificates issued by the State Enterprise Centre of Registers.

The State Enterprise Centre of Registers refused to comply and challenged the administrative order in the court. The plaintiff was successful in the administrative court of first instance (the Vilnius District Administrative Court) in that the order was annulled. The State Data Protection Inspectorate appealed this decision, and brought the case to the final instance of administrative justice (the Higher Administrative Court of the Republic of Lithuania).

Arguments of the court

The court emphasized that the legal interpretation relies on the factual acknowledgment that the use of the personal identification number in the qualified electronic signature certificate discloses the personal identification number to the recipient (addressee) of the electronic documents signed with the public certificate. Furthermore, where the signed electronic documents are further distributed by the recipient, this also causes further publicity of the personal identification number.

The court held that the Law on Legal Protection of Personal Data is a special law with respect to the Law on Electronic Signatures, hence the rules of the former supersede any rules of the latter. Specifically, the Law on Electronic Signatures does not provide any exceptions from the special rules of personal identification number processing, according to the Law on Legal Protection of Personal Data.

The court also suggested a test for verifying whether the personal data processing meets the general principle of using only a minimum of personal data required for the purpose – if the same purpose of data processing can be achieved without using a disputed data item, then the processing of such a data item shall be deemed excessive. Thus, in a specific situation, while the processing of personal data is justifiable for the State Enterprise Centre of Registers own purposes of identifying the signatory, it is not justifiable to incorporate the personal identification number into the public qualified electronic signature certificate, which is distributed to other parties. In order for the latter use of the personal identification number to be acceptable, the consent of the data subject is mandatory, according to the article 7 of the Law on Legal Protection of Personal Data.

Moreover, article 7 of the Law on Legal Protection of Personal Data imperatively prohibits making the personal identification number public. The factual aspect of inadvertent dissemination of the personal identification number through the communicating of the signed electronic documents (with the public qualified certificate attached) constituted an infringement of this imperative.

On the basis of the above, the Higher Administrative Court of the Republic of Lithuanian reversed the decision of the first instance and upheld the administrative order of the State Data Protection Inspectorate.

Implications

The case and the arguments of the court have revived the discussion on the privacy issues relating to personal identifications numbers in Lithuania. Currently plans are being laid down to phase out the existing personal identification number nomenclature and to replace it with the random string of 11 digits.

Nevertheless, the privacy friendly decision of the court may prove to be Pyrrhic victory, since the State Enterprise Centre of Registers has not abandoned the practice of incorporating the personal identification number into the public qualified certificated as of yet. Moreover, in the latest development as of September 2014, it is likely that the decision of the court will be at least partially overruled by the new legislation, mandating the inclusion of personal identification numbers into the public qualified electronic signature certificates, which are submitted to the Register of Legal Entities (which is also run by the State Enterprise Centre of Registers).

Mindaugas Kiškis is professor of law and management at the Institute of Digital Technology, Mykolas Romeris University, Lithuania. His research interests include intellectual property, privacy, data protection, technology law and policy, innovation and entrepreneurship. He has been a member of several committees drafting legislation regarding privacy, intellectual property and media.

http://www.kiskis.eu

mindaugas@kiskis.eu