LEXOLOGY

Global, Latvia July 27 2016

Valts Nerets (Senior Associate) and **Agita Sprūde** (Associate)

SORAINEN

http://www.lexology.com/library/detail.aspx?g=f619dc4c-cf2b-4b48-9909-00e37dc75859

Jurisdiction snapshot

- *Trends and climate*

Would you consider your national data protection laws to be ahead or behind of the international curve?

The Personal Data Protection Law is in line with the international curve. The Latvian legislature follows international trends in personal data protection, but is not proactive. The state institution responsible for supervising the protection of personal data is the Data State Inspectorate (DSI). To a large extent, its recommendations for personal data protection follow the opinions drafted by the Article 29 Data Protection Working Party.

- **Are any changes to existing data protection legislation proposed or expected in the near future?**

The latest amendments to the Personal Data Protection Law were enacted in February 2014, and

no new amendments are expected in the near future. In May 2016 minor technical amendments were adopted through regulations of the Cabinet of Ministers on the application templates for the registration of personal data processing and personal data protection specialists.

- **Legal framework**

- *Legislation*

What legislation governs the collection, storage and use of personal data?

The collection, storage and use of personal data is governed by the Personal Data Protection Law, which came into force on April 20 2000, as amended and regulations of the Cabinet of Ministers issued pursuant to the authorisation granted under the Personal Data Protection Law.

- *Scope and jurisdiction*

Who falls within the scope of the legislation?

The law mainly imposes obligations on data controllers. The data processor must use the necessary technical and organisational measures to:

- protect personal data;
- prevent illegal processing; and
- process personal data in accordance with the instructions and restrictions given by the data controller.

- The Personal Data Protection Law applies to the processing of all types of personal data and to any natural person or legal person if:
  - the data controller is registered in Latvia;
  - data processing is performed outside the borders of Latvia in territories which belong to Latvia in accordance with international agreements; or
  - equipment used for the processing of personal data is located in Latvia, except where it is used only to transfer personal data via Latvia.

- **What kind of data falls within the scope of the legislation?**

The law defines 'personal data' as "any information related to an identified or identifiable natural person". The Data State Inspectorate (DSI) has adopted guidance on the definition of personal

data that is similar to Opinion 4/2007 on the concept of personal data of the Article 29 Data Protection Working Party. IP addresses are also considered to be personal data.

- **Are data owners required to register with the relevant authority before processing data?**

Latvia has no requirement to register databases that contain personal data or to register as a personal data processor, either generally or for specific categories of data. However, data processing itself, as a process or action, may be subject to registration with the DSI by the data controller.

- Before commencement of processing of personal data, the data controller must register the processing of personal data with the DSI or assign a natural person (ie, a data protection specialist) if the data controller:

  - intends to transfer personal data to a state other than a member state of the European Union or the European Economic Area;
  - intends to process personal data when:
    - providing financial or insurance services;
    - carrying out raffles or lotteries, market or public opinion researches, personnel selection or personnel assessment; or
    - providing debt recovery services and credit information processing services;
  - carries out processing of sensitive personal data, except for cases where the data processing is carried out for the purposes of accounting or personnel registration (employment legal relations), or if it is carried out by religious organisations;
  - processes personal data in relation to criminal offences, criminal records or penalties in administrative violations;
  - carries out video surveillance retaining personal data; or
  - carries out processing of genetic data.

- Even in the cases mentioned above, data processing registration is not required if the data controller has registered its personal data protection specialist with the DSI. Under Latvian law, a 'data protection specialist' is a natural person who has obtained qualifications in the fields of law, IT or similar and who has passed an exam pursuant to an order prescribed by the Cabinet of Ministers. The data protection specialist is not the personal data processor.

- **Is information regarding registered data owners publicly available?**

Yes, the personal data processing register is available online. However, in general the register shows only that the particular data controller has registered some data processing activities. If more information is needed, this must be requested from the DSI in writing. The information will be provided within one month. A register of personal data protection specialists is available at www.dvi.gov.lv/lv/personas-datu-apstrades-un-specialistu-registracijas-kartiba/personas-datu-aizsardzibas-specialisti/.

- **Is there a requirement to appoint a data protection officer?**

If the Personal Data Protection Law applies, appointing a data protection specialist is an alternative to registering the personal data processing. Otherwise, the data controller is not required to have a data protection specialist.

- *Enforcement*

Which body is responsible for enforcing data protection legislation and what are its powers?

The supervision of personal data protection is carried out by the DSI, which is part of the Ministry of Justice. The DSI operates independently and fulfils the functions specified in law by taking decisions and issuing administrative acts. The DSI is managed by a director who is appointed and released from his or her position by the Cabinet of Ministers, pursuant to the recommendation of the minister for justice.

- **Collection and storage of data**

- *Collection and management*

In what circumstances can personal data be collected, stored and processed?

The Personal Data Protection Law provides that personal data may be processed only if:

- the data subject has given consent;
- a contract to which the data subject is party is being concluded or performed;
- the data controller has a legal obligation to process personal data;
- processing is necessary in order to protect vital interests of the data subject;

- processing is necessary for the exercise of official authority vested by laws and other legal acts in state and municipal institutions, agencies, enterprises or a third party to which personal data is disclosed; or
- data processing is necessary for the purposes of legitimate interests pursued by the data controller or a third party to which the personal data is disclosed, unless such interests are overridden by interests of the data subject.

- **Are there any limitations or restrictions on the period for which an organisation may (or must) retain records?**

There are no generally applicable timelines for retaining records. Personal data may be processed only for as long as is required for the purposes of the processing.

- **Do individuals have a right to access personal information about them that is held by an organisation?**

Yes, an individual has a right to access all information collected about him or her that is held by an organisation and to obtain information about parties which have accessed that personal data unless the personal data was accessed by law enforcement authorities or for the purposes of a criminal investigation.

- **Do individuals have a right to request deletion of their data?**

Yes, if such personal data is incomplete or inaccurate in accordance with the purpose of the personal data processing. The data subject may also demand the correction of his or her inaccurate personal data.

- *Consent obligations*

Is consent required before processing personal data?

Yes, unless data is processed on another basis permitted by law.

- **If consent is not provided, are there other circumstances in which data processing is permitted?**

Yes, but only if personal data is processed:

- to fulfil a contract to which the data subject is party;

- based on a law requiring the processing of personal data;
- in order to protect the interests of the data subject;
- when exercising the official authority vested by laws and other legal acts in state and municipal institutions, agencies, enterprises or a third party to which personal data is disclosed; or
- to protect the legitimate interests of the data controller or a third party to which personal data is disclosed, unless such interests are overridden by interests of the data subject.

- The processing of sensitive personal data (ie, personal data which indicates the race, ethnic origin, religious, philosophical or political convictions or trade union membership of a person, or provides information as to the health or sexual life of a person) is generally prohibited unless special exemptions provided by law apply.

- **What information must be provided to individuals when personal data is collected?**

If data processing is based on consent, the individual must be provided with:

- the name and address of the data controller; and
- the intended purpose of the personal data processing.

- If requested by the data subject, the data controller must provide the following information:

- the possible recipients of the personal data;
- the right of the data subject to gain access to his or her personal data and to correct such data;
- whether providing an answer is mandatory or voluntary, as well as the possible consequences of failing to provide an answer; and
- the legal basis for the processing of personal data.

- If the data processing is based on law, the same rules apply as where data processing is based on consent, unless the law specifically authorises the processing of personal data without disclosing the purpose.

- **Data security and breach notification**

- *Security obligations*

Are there specific security obligations that must be complied with?

Personal data processing must meet certain technical and organisational requirements set by the Cabinet of Ministers Regulations on Mandatory Technical and Organisational Requirements for Personal Data Protection. Under Latvian law there are no specific requirements for certain categories of personal data, and no regulatory requirements for cloud service providers. The data controller must adopt internal regulations for the processing of personal data, in order to classify the personal data protection pursuant to the value and confidentiality level of the data.

- The law also provides that personal data must be protected by passwords and encryption, and states which information must be stored on the receipt and transfer of personal data:

  - the time of transfer;
  - the parties involved; and
  - the data processed.

- Further, in its internal data processing regulations the data controller must determine the length of the password and the rules for its creation. However, the minimum length of the password is eight letters. The technical protection of personal data must be ensured by physical and other means (eg, passwords or encryption). The data controller must also ensure, for example, that:

  - personal data is accessed only by authorised persons;
  - certain information is stored when a personal data transfer takes place; and
  - internal personal data protection regulations are drafted.

- *Breach notification*

Are data owners/processors required to notify individuals in the event of a breach?

No, only electronic communications merchants have a mandatory obligation to notify individuals in the event of a breach.

- **Are data owners/processors required to notify the regulator in the event of a breach?**

Yes, in the event of a breach the electronic communications merchant must notify the Data State Inspectorate of the circumstances and type of breach immediately. The merchant must keep the

information regarding the type of the breach, its consequences and actions taken, as well as information on when and to whom it has provided data regarding the breach, for 18 months.

- **Electronic marketing and internet use**

- *Electronic marketing*

Are there rules specifically governing unsolicited electronic marketing (spam)?

Yes. Although the Personal Data Protection Law does not specifically address (electronic) marketing, it contains provisions stating that data subjects have the right to prohibit the use of their personal data for marketing purposes. Moreover, the provisions on electronic marketing are also included in the Law on Information Society Services, which requires prior express consent (the opt-in approach) from the data subject before using his or her contact information (eg, email address or phone number) for electronic marketing purposes. In practice, a checkbox separate from the acceptance of the standard terms is often used to obtain this consent.

- According to the Law on Information Society Services, no consent is required if:
  - the data has been obtained in the course of the sale of goods or provision of services and is used for the same or similar goods or services;
  - the recipient is able to refuse the use of the personal data easily and at no cost; and
  - the recipient has not previously declared that he or she does not want to be contacted.

- *Cookies*

Are there rules governing the use of cookies?

Yes, the use of cookies is governed by the Law on Information Society Services (effective December 1 2004), which is available online at www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_Information_Society_Services.doc(unofficial English translation).

- **Data transfer and third parties**

- *Cross-border data transfer*

What rules govern the transfer of data outside your jurisdiction?

The Personal Data Protection Law governs the transfer of data outside Latvia. If the data controller intends to transfer personal data to a state other than a member state of the European Union or the European Economic Area, before the transfer it must register personal data

processing with the Data State Inspectorate (DSI) or assign and register with the DSI a data protection specialist.

- **Are there restrictions on the geographic transfer of data?**

Yes, personal data may be transferred outside the European Union or European Economic Area if that state provides the same level of data protection as in Latvia (the adequate protection requirement). According to the DSI, approved states include Australia, Canada, Israel and the Isle of Man. Since October 6 2015 the safe harbour scheme is no longer considered to provide adequate protection.

- The transfer of personal data to other states is permissible if the data controller undertakes to supervise the performance of the relevant protection measures, or at least one of the following conditions is complied with:

  - the data subject's consent has been obtained;
  - the transfer of the data is necessary in order to fulfil an agreement between the data subject and the data controller, the personal data is required to be transferred in accordance with contractual obligations binding on the data subject or, taking into account a request from the data subject, the transfer of data is necessary in order to enter into a contract;
  - the transfer of data required and requested, pursuant to prescribed procedures, in accordance with significant state or public interests or for judicial proceedings;
  - the transfer of the data is necessary to protect the life and health of the data subject; or
  - the transfer of the data concerns personal data that is public or has been accumulated in a publicly accessible register.

- The data controller's supervision of the relevant protection measures as a pre-condition for the personal data transfer may be carried out by ensuring that:

  - the data controller enters into a contract regarding transfer of the data according to the contractual provisions set by the Cabinet of Ministers;
  - the data controller is bound by binding regulations of a company, containing principles for processing and protection of personal data, which guarantee the rights of data subjects and are approved by a personal data protection supervision institutions of an EU member state; or

- the data controller enters into the contract in conformity with standard clauses of a contract regarding the transfer of personal data to third countries approved by the European Commission.

- *Third parties*

Do any specific requirements apply to data owners where personal data is transferred to a third party for processing?

The key principle under the Personal Data Protection Law is that data processing be carried out with a legitimate aim, taking into account the purpose of processing, the period of processing and other criteria. The processing of personal data is permitted if:

- the data subject has given his or her consent;
- the processing of data results from contractual obligations of the data subject or, taking into account a request from the data subject, the processing of data is necessary in order to enter into the relevant contract;
- the processing of data is necessary for a data controller to perform its legal duties;
- the processing of data is necessary to protect important interests of the data subject, including life and health;
- the processing of data is necessary in order to comply with public interest or to exercise functions of public authority for whose performance the personal data has been transferred to a data controller or transmitted to a third person; or
- the processing of data is necessary in order to, in compliance with the fundamental human rights and freedoms of the data subject, exercise lawful interests of the data controller or of such third person to which the personal data has been disclosed.

- The data controller is solely responsible for the compliance of the data processing with data protection laws, including processing carried out by third parties which receive the personal data from the data controller for processing. The restrictions on the geographic transfer of data also apply to the transfer of personal data to third parties for processing.

- **Penalties and compensation**

- *Penalties*

What are the potential penalties for non-compliance with data protection provisions?

The violation of data protection rules or the breach of the rights of the data subject is a punishable offence under the Administrative Violations Code. For illegal actions related to personal data (including collecting, organising, classifying, editing, storing, using, transferring, disclosing, blocking or erasing of the personal data) or for a violation of the data protection rules, a fine of up to €11,400 and the possible confiscation of the objects used to commit the violation may be imposed. If the offence is committed with regard to sensitive data or repeatedly, a fine up to €14,000 may be imposed.

- Criminal penalties apply to unlawful actions involving personal data if the action causes serious harm or is carried out by the controller or processor for the purpose of blackmail, to gain monetary benefit or for revenge. However, these are enforced only in extremely rare cases.

- *Compensation*

Are individuals entitled to compensation for loss suffered as a result of a data breach or non-compliance with data protection provisions by the data owner?

There is no pre-determined compensation prescribed in the applicable legal acts. Individuals may present a civil claim for damages to the data controller.

- **Cybersecurity**

- *Cybersecurity legislation, regulation and enforcement*

Has legislation been introduced in your jurisdiction that specifically covers cybercrime and/or cybersecurity?

Yes, the Law on the Security of Information Technologies applies.

- **What are the other significant regulatory considerations regarding cybersecurity in your jurisdiction (including any international standards that have been adopted)?**

Latvia follows EU policy in the field of cybersecurity. No specific international standards have been adopted. Latvia is a party to the Budapest Convention on Cybercrime (2001).

- **Which cyber activities are criminalised in your jurisdiction?**

The following activities have been criminalised:

- the illegal alteration, deletion, damaging or blocking of data in computer systems;
- the unlawful removal or alteration, for commercial purposes, of the means of identification of terminal equipment used in an electronic communication network;

- illegal interference with or hindering of the functioning of computer systems by way of uploading, transmitting, deleting, damaging, altering or blocking of data;
- proprietary damage to another person through unlawful entry, alteration, deletion, damaging or blocking of computer programs or data or other unlawful interference with data processing operation for the purpose of proprietary benefit;
- the supply, production, possession, distribution or otherwise making available of a device or computer program which is created or adjusted for the commission of criminal offences specified in the Penal Code, or of means of protection which allow access to a computer system with the intention of committing or enabling a third person to commit crimes specified in the Penal Code;
- the illegal accessing of computer systems by elimination or avoidance of means of protection;
- illegal access to communications sent via electronic channels or the breach of communications privacy or illegal access to confidential data or illegal capture of signals sent in electronic communications channels;
- the use of terminal equipment with unlawfully removed or altered means of identification in an electronic communications network by a person who is aware that the identification code has been unlawfully removed or altered; or
- offences against intellectual property (eg, infringement of copyright in computer systems, trade in pirated goods, copyright infringement, illegal receipt of information society or media services or the removal of technical protective measures and information).

- **Which authorities are responsible for enforcing cybersecurity rules?**

The Information Technologies Security Incidents Response Institution (known as 'cert.lv') promotes the security of information technology. Certain functions are delegated to the Institute of Mathematics and the Computer Science of the University of Latvia.

- The state police, the security police and the Prosecutor's Office are responsible for investigating and prosecuting criminal matters.

- *Cybersecurity best practice and reporting*

Can companies obtain insurance for cybersecurity breaches and is it common to do so?

Insurance for cybersecurity breaches is rare in Latvia and the availability of such insurance is limited.

- **Are companies required to keep records of cybercrime threats, attacks and breaches?**

There are no requirements for keeping records of cybercrime threats, attacks and breaches.

- **Are companies required to report cybercrime threats, attacks and breaches to the relevant authorities?**

Only the state or local government authorities, owners or lawful possessors of critical IT infrastructure and electronic communications merchants must report personal data threats, attacks or breaches to the Data State Inspectorate. There is no general obligation to report cybercrime threats, attacks or breaches to the relevant authorities. However, cert.lv can request and receive from state and local government authorities and other legal persons technical information regarding an IT security incident (eg, information on the scope of the incident, malicious software files that have caused the incident, a description of vulnerabilities, technical measures performed for the prevention of the incident, information regarding activities performed by persons doing harm or other technical information, including IP addresses), as well as obtaining, by mutual agreement, online data flow.

- **Are companies required to report cybercrime threats, attacks and breaches publicly?**

No. cert.lv may inform the public or require the relevant electronic communications merchants to do so if it determines that disclosure of the breach is in the public interest.

- *Criminal sanctions and penalties*

What are the potential criminal sanctions for cybercrime?

The penalty depends on the crime and its gravity. For natural persons the penalty is usually a fine or imprisonment, while for legal persons the penalty is a confiscation of property or a fine.

- **What penalties may be imposed for failure to comply with cybersecurity regulations?**

The penalty depends on the crime and its gravity. For natural persons the penalty is usually a fine or imprisonment for up to seven years. In case of a legal person, the court may order the confiscation of property or a fine of up to €75,000 minimal wages (the Latvian minimum wage is currently €370).