Human Rights Monitoring Institute

The Preparedness of Lithuanian Businesses to

IMPLEMENT THE GENERAL DATA PROTECTION REGULATION

About the Human Rights Monitoring Institute

The Human Rights Monitoring Institute (HRMI) is a non-governmental, non-profit public advocacy organization. Since its establishment in 2003, HRMI has been advocating for full compliance of national laws and policies with international human rights obligations.

The team of HRMI legal and public policy experts carries out research, proposes legislation and policy documents, participates in working groups, compiles reports to international human rights bodies, undertakes strategic cases before domestic and international courts, provides expert consultations and legal services, engages in various national and international projects, delivers conventional and distance training (via the beribu.lt platform) to law enforcement officers and other public authorities.

The HRMI is active in the fields of: rights of the victims of crime, rights of suspects and the accused, prohibition of discrimination, protection of privacy and digital rights, freedom of expression, human rights and corporate social responsibility.

www.hrmi.lt

About the study

Authors: dr. Mindaugas Kiškis
("The preparedness of Lithuanian businesses to implement the Regulation"; "Summary")

Natalija Bitiukova and Karolis Liutkevičius
("Preface", "The current regulatory regime governing the protection of personal data in Lithuania" and "Changes introduced by the General Data Protection Regulation that are relevant to busiensses")

Translation: Petras Borisovas

The study is a part of HRMI's initiative „Digital Rights"

The study was funded by the EEA Grants 2009-2014 NGO Programme Lithuania. The Human Rights Monitoring Institute assumes full responsibility for the contents of this publication. The contents of this publication should not be seen as reflecting the views of the donor.

If you wish to receive the data of the survey in another format, please contact us by e-mail at hrmi@hrmi.lt.

Definitions

LLPPD – the Law on Legal Protection of Personal Data of the Republic of Lithuania.

Personal data – any information relating to a natural person whose identity has been identified or could be identified with reference to said data. This covers a person's name, personal identification code, date of birth, fingerprints, biometric data, IP address and other identifiers.

General Data Protection Regulation – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.[1]

Data Protection Directive – 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.[2]

Data Protection Reform – a set of legislative proposals put forth by the European Commission in 2012 to update and modernize the rules laid out in the Data Protection Directive (1995) and the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (2008).

Data subject – a natural person whose data is being processed.

Processing – a broad concept covering any and all operations performed on personal data, such as collection, recording, organizing, storage, classification, grouping, combination, alteration, disclosure, publication, use, logical or arithmetic operations, retrieval, dissemination, destruction et al.

Processor – a natural or legal person which processes personal data on behalf of the controller.

Controller – a natural or legal person which determines the purposes and means of the processing of personal data.

Supervisory authority – an independent public authority established by a Member State and responsible for supervising the implementation of the Regulation. In Lithuania, this would be the State Data Protection Inspectorate (SDPI)

Profiling – any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, such as his or her performance at work, economic situation, health, personal preferences, interests, reliability and others.

[1] Official text: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=LT [all links were checked and reported working on 7 September 2016]

[2] Official text: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=LT

Content

Preface

The EU Charter of Fundamental Rights recognizes the right of every person to the protection of personal data concerning him or her. The Charter provides that personal data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or other legitimate basis laid down by law."[3]

For a long time, this right was regulated under the 1995 Data Protection Directive.[4] However, in the context of exponential technological advancement, experts quickly became aware that this legal instrument failed to address the challenges faced by digital society on a daily basis and in some cases even stifled innovation.

To account for these developments, the European Commission began the so-called Data Protection Reform, the crux of which was the General Data Protection Regulation.[5] Adopted in April of 2016, this regulation aims to create a more favourable business environment by establishing common data protection rules for all business entities operating in the EU market.[6]

According to the European Commission, "[a] single law will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. The initiative will help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe."[7]

The Regulation eases the administrative burden on companies and allows them to independently assess the risks related to their operations. On the other hand, it places stricter obligations on companies with regards to data protection by setting up a high standard for accountability, covering impact assessment, the appointment of data protection offices and notification of data breaches. Companies in violation of the personal data protection rules can now expect to see fines of up to €20 million or up to 4% of their total turnover for the preceding financial year.

[3] EU Charter of Fundamental Rights, 26 October 2012, 2012/C 326/02, Art. 8, http://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A12012P%2FTXT

[4] 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 L 281, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=LT

[5] European Commission, „Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses", *Europa.eu*, 25 January 2012, http://europa.eu/rapid/press-release_IP-12-46_lt.htm
The second instrument of the Data Protection Reform package is Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or persecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. This directive shall not be discussed further.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[7] European Commission, „Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses", *Europa.eu*, 25 January 2012, http://europa.eu/rapid/press-release_IP-12-46_lt.htm

About the study

This study has two primary aims:

1

To assess

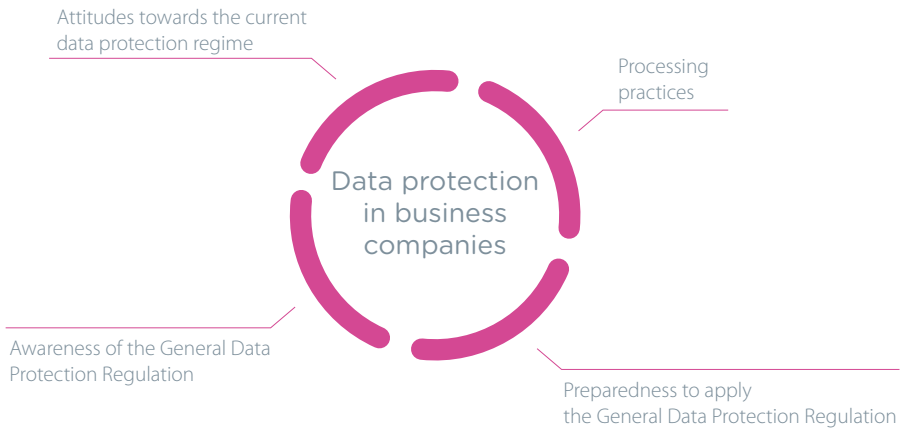
the preparedness of Lithuanian businesses to implement the provisions of the General Data Protection Regulation

2

To raise

awareness of the changes brought about by the General Data Protection Regulation that are pertinent to businesses

To assess the prevailing attitudes among business entities, the Human Rights Monitoring Institute, in collaboration with "Sprinter research", conducted an exploratory survey of 50 Lithuanian companies in July 2016, asking participants questions about data protection in the four key areas:



To provide structured information on the provisions of the General Data Protection Regulation to professionals working in the field of data protection (lawyers, IT professionals, data protection and compliance officers, NGO staff), we compared the current data protection scheme with the changes that will soon be applied.

This review of the changes brought about does not cover the whole Regulation – for example, Chapter III of the Regulation (rights of the data subject) is explored in-depth in another study prepared by Human Rights Monitoring Institute, titled "The Privacy Paradox: The Lithuanian Public's Perceptions of Data Protection."[8] It should be noted that this study focuses on situations where data controllers and processors are business companies and not state authorities.

[8] www.hrmi.lt. Also, this study does not cover international transfers of personal data. Rules for such transfers are provided under Chapter V of the Regulation.

The current regulatory regime governing the protection of personal data in Lithuania

The primary law guaranteeing the right to personal data protection in Lithuania is the Law on Legal Protection of Personal Data (LLPPD), adopted way back in 1996.[9] The law was later amended to incorporate the provisions of Directive 95/46/EC of the European Parliament and of the Council (on the protection of individuals with regard to the processing of personal data and on the free movement of such data) into the Lithuanian legal system.[10]

LLPPD applies to situations where legal entities (for example, business companies) or natural persons (for example, individual businessmen) process personal data for business or professional purposes. These entities are referred to as controllers or processors.[11] LLPPD does not apply in situations where natural persons process personal data for their private purposes – for example, entering friends' addresses and dates of birth into an *Excel* document.[12]

The LLPPD specifies that personal data is any information relating to a natural person whose identity has been identified or could be identified with reference to said data.[13] This could be their name, personal identification code, date of birth, fingerprints, biometric data or even their IP address.[14] The LLPPD distinguishes special personal data from all other personal data, prohibiting its processing except for the circumstances outlined in the act.[15] Special personal data is data relating to the natural person racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life or criminal record.[16]

Persons whose personal data is being processed are called data subjects.[17] Only natural persons may be referred to as data subjects– the LLPPD does not apply when processing the data of legal entities, since such data, by its very nature, is not personal data.[18]

9 Law No. I-1374 on Legal Protection of Personal Data, 11 June 1996, https://www.e-tar.lt/portal/lt/legalAct/TAR.5368B592234C/lGOrBAvuZc

10 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 L 281, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=LT

11 Art. 2(6)-(7) of LLPPD

12 Art. 1(4) of LLPPD

13 Art. 2(1) of LLPPD

14 State Data Protection Inspectorate, „Is an IP address personal data?", https://www.ada.lt/images/cms/File/naujienu/Ar%20IP%20adresas%20yra%20asmens%20duomenys.pdf.

15 Data related to the person's racial or ethnic origin, political opinions, religious, philosophical or other beliefs, trade union membership, health, sexual life as well their criminal record is considered to be special data and subject to additional safeguards (Art 2(8) and 5(2) of LLPPD)

16 Art. 5(2) of LLPPD

17 Art. 2(8) of LLPPD

18 In this study, "data subject", "person" and "resident" are used interchangeably unless noted otherwise.

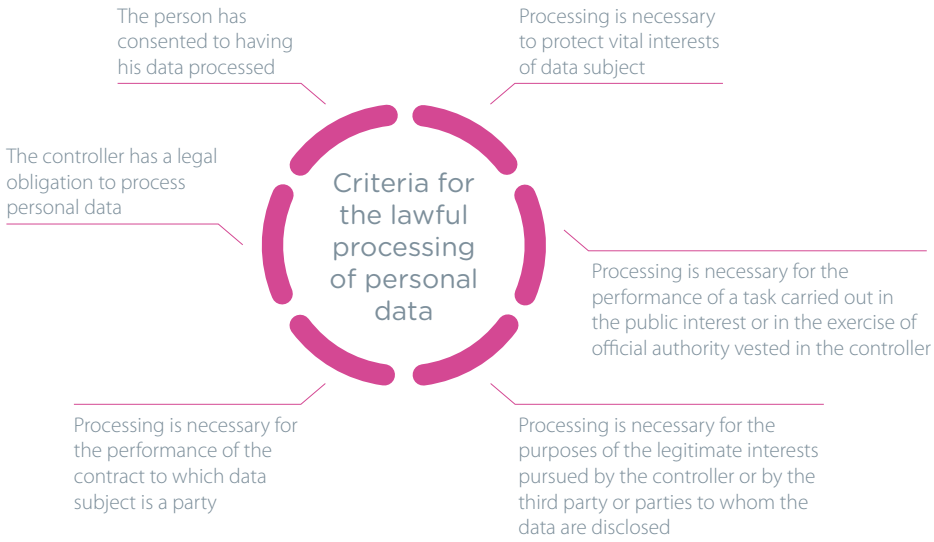
The European Court of Justice has ruled that legal entities may only avail themselves of the right to data protection when it comes their name, if it can be used to identify one or more natural persons (*Volker and Markus Schecke and Hartmut Eifert v. Land*, C-92/09 and C-93/09, 9 November 2010, para. 52).

Processing is defined in very broad terms, covering any and all operations performed on personal data, such as collection, recording, organizing, storage, classification, grouping, combination, alteration, disclosure, publication, use, logical or arithmetic operations, retrieval, dissemination, destruction et al.[19]

Processing is only lawful if it based on one or more of the six grounds (criteria) for lawful processing specified in the LLPPD.[20] The LLPPD also sets out the requirements for processing and the rules that controllers and processors must follow.[21]

The first step that any company wishing to process personal data needs to take is to notify the State Data Protection Inspectorate (SDPI) about it.[22] In some cases, the SDPI may have to do some prior checking before to entering the controller into the State Personal Data Controllers Register personal data controllers state register.[23]

Articles 214(14) and 214(16) of the Code on Administrative Violations of Law set out liability for breaches of the LLPPD, such as when a company collects data without the data subject's consent and absent any other lawful processing criterion.[24] Fines for unlawfully processing of data or violating the data subject's rights range from €144 to €579.[25]



19 Art. 2(4) of LLPPD
20 It should be noted that especially sensitive (special) data is subject to different processing criteria, see Art. 5(2) of LLPPD
21 Section II of LLPPD
22 Art. 31 of LLPPD
23 Art. 33 of LLPPD
24 Code of Administrative Violations of Law, 13 December 1984, No. X-4449, https://www.e-tar.lt/portal/lt/legalAct/TAR.FC2B71C84492/TAIS_495174
25 *Ibid.*

Changes introduced by the General Data Protection Regulation that are relevant to businesses

Since 1995, the rights of data subjects at EU level were regulated by the aforementioned Data Protection Directive. Eventually, the legal framework created in the last century was no longer able to meet the expectations of digital society and cope with new data protection challenges. Data collection and data sharing increased significantly in scope, while economic and social integration lead to greater cross-border data traffic.

> In 1995, only 1% of the world's population had access to the Internet; today, more than 40% regularly connect to the World Wide Web.[26] The *Google* search engine, which nowadays carries out up to two trillion searches a year, only became operational in 1996.[27]

In order fully account for these developments and promote the digital economy, the European Commission launched the so-called Data Protection Reform, the crux of which was the General Data Protection Regulation.[28] The Regulation was finally adopted in the April of 2016, after nearly four years of negotiations between the European Commission, the Council, the European Parliament and business representatives, non-governmental organizations and other interested parties.[29] The Regulation will be applied from 25 May 2018, giving both Member States and businesses time to prepare for its implementation.[30]

Before we move on to discuss its provisions, it is important to note that, unlike the Data Protection Directive, the Regulation is directly applicable. This means that there is no need to transpose its provisions into national law and that it has legal effect from its entry into force. However, the Regulation gives discretion to the Member States in certain areas – that is, they can choose how legal relations shall be regulated. For example, the Regulation provides that Member States may restrict proportional restrictions on data subjects' rights into national law, when such restrictions are necessary for the purposes of national security, defense, prevention of crime and the like.[31]

It is estimated that the Regulation contains more than fifty such "flexible" provisions,[32] so it is likely that before it enters into force there will be changes in Lithuania's personal data protection regime. In any case, national legislation that is in conflict with the Regulation shall cease to apply on 25 May 2018.

What follows is an overview of the main changes introduced by the Regulation for controllers and processors. Data subjects' rights and corresponding obligations placed on controllers is explored in-depth in another study prepared by the Human Rights Monitoring Institute, titled "The Privacy Paradox: The Lithuanian Public's Perceptions of Data Protection."[33]

26 Internet users in the world (live statistics): http://www.internetlivestats.com/internet-users/
27 Danny Sullivan, "Google now handles at least 2 trillion searches per year", *Searchengineland.com*, 24 May 2014, http://searchengineland.com/google-now-handles-2-999-trillion-searches-per-year-2502477
28 European Commission, „Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses", *Europa.eu*, 25 January 2012, http://europa.eu/rapid/press-release_IP-12-46_lt.htm
29 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC
30 Art. 99(2) of the Regulation
31 Art. 23 of the Regulation
32 https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf
33 www.hrmi.lt

Scope of the Regulation

The Regulation preserves the fundamental provisions of the Directive and, by extension, the LLPPD. Personal data may only be processed if there are legitimate grounds (criteria) for doing so, with these grounds being essentially the same as before, and it must comply with data processing principles.[34] The Regulation retains the prohibition on processing special (called "sensitive" in the Regulation) data, unless an exception applies. The category of sensitive data has been expanded to include genetic and biometric data.[35]

One of the most prominent changes is the expansion of the scope of the Regulation. The LLPPD applies to businesses that have been established and are operating in Lithuania, while the Regulation applies to business entities established in any EU country, irrespective of whether the data itself is being processed in EU territory. The greatest change is that the Regulation provides for the so-called "extraterritorial application" – that is, even business entities that have been established outside the EU (e.g. in the US, Brazil, China) must comply with the Regulation if they do one of the following:[36]

- offer free or paid goods and services to EU residents (e.g. e-shops, loyalty scheme platforms). Whether the goods and services are actually "directed at" at EU residents may be determined based on the following aspects: the language settings of the website offering goods (e.g. a US site allows visitors to view the information in Hungarian or Bulgarian); payment options (e.g. the site can display prices in euros); ability to ship to the EU; customer base (e.g. EU residents are the largest group among the site's customers) et al.[37]
- Monitor the behavior of data subjects in the EU (e.g. using apps to track an individual's location; tools to track individuals across multiple sites)

Such business entities should appoint a representative to a Member State,[38] whose primary function would be to communicate with EU data protection supervisory authorities.[39]

[34] Art. 5 and 6 of the Regulation. Still, the Regulation sets out stricter requirements for obtaining consent from the data subject, see. "The Privacy Paradox: The Lithuanian Public's Perceptions of Data Protection"

[35] Art. 9 of the Regulation

[36] Art. 3 of the Regulation.

[37] Linklaters, "The General Data Protection Regulation: a survival guide", *Linklaters.com*, 2016, p. 27, http://www.linklaters.com/pdfs/mkt/london/TMT_DATA_Protection_Survival_Guide_Singles.pdf

[38] This obligation shall not apply when processing is occasional, does not include, on a large scale, processing of special categories of data, or processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing (Art. 27(2) of the Regulation)

[39] Art. 9 of the Regulation; see analogy with Art. 1(3)(3) of LLPPD

The accountability principle

The accountability principle is one of the most fundamental changes brought about by the Regulation – in fact, it may be considered to lie at the very core of it. The principle, at its heart, seems simple enough, but it is exceedingly difficult or even impossible to implement in practice without further preparation, consultation with data protection specialists or without committing more human resources or funds. The accountability principle goes like this: "[t]he controller shall be responsible for, and be able to demonstrate compliance with, [data processing principles]".[40] To properly implement this principle, data protection must become an integral part to the company's activities, from the inception of goods or services to the point where the client's data is destroyed.

Below are several measures laid down by the Regulation that help uphold the accountability principle:

- **Data protection by design (also known as privacy by design) and by default (privacy by default).** It is expected that controllers, when selecting processing measures and when processing data, implement appropriate "technical and organizational measures", which are designed to implement data protection principles.[41] As an example of one such measure, the Regulation proposes pseudonymisation, which translates to the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately.[42]

- **Records of processing activities.** Companies will have to store documents relating to processing operations and provide them upon receiving a request from the supervisory authority. This information covers descriptions of the categories of data subjects and of the categories of personal data, the categories of recipients of data, envisaged time limits for storage and others. This obligation applies to both controllers[43] and processors,[44] albeit to a different degree.

- **Security of processing.** Just like the LLPPD,[45] the Regulation places a sufficiently broad obligation on companies[46] to "implement appropriate technical and organizational measures" to ensure that the data is protected against unauthorized destruction, disclosure, transmission and so on. The Regulation provides several examples of "appropriate" measures (pseudonymisation, data encryption, confidentiality of processing systems et al.), but they must be selected on a case-by-case basis, taking into account the likelihood and severity of risk.[47] The Regulation also requires controllers to notify data supervisory authorities about personal data breaches that pose a threat to the rights of persons.[48] When the personal data breach is likely to result in a high risk to the rights of natural persons, then it must be communicated to the data subject.[49] In Lithuania, only telecommunications companies, Internet service providers and other companies providing electronic communications services,[50] as well managers of critical informational infrastructures[51] and other such entities are under an obligation to report data breaches to the SDPI on certain occasions. By contrast, the Regulation places this requirement on all companies and institutions that process data, irrespective of the nature of their operations.

40 Art. 5(2) of the Regulation

41 Art. 25 of the Regulation

42 Art. 4(5) of the Regulation

43 Art. 30(1) of the Regulation. The information that controllers must provide data subjects with is largely the same (Art. 13(1) of the Regulation)

44 Art. 30(2) of the Regulation

45 Art. 30 of LLPPD

46 Both data controllers and data processors are subject to this obligation.

47 Art. 32 of the Regulation

48 Meanwhile, the processor is under an obligation to report security breaches to the controller (Art. 33 of the Regulation)

49 For more information, see „The Privacy Paradox: The Lithuanian Public's Perceptions of Data Protection."

50 Art 62(4) of the Law No. IX-2135 on Electronic Communications, 15 April 2004, https://www.e-tar.lt/portal/lt/legalAct/TAR.82D8168D3049/BWaAwPRnRd

51 Art 11(4) of the Law No. XII-1428 on Cyber Security, 23 December 2014, https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4

- **Data protection impact assessment.** Where processing is likely to result in a high risk to the rights of natural persons, the controller must first carry out a data protection impact assessment. The assessment must include a description of the envisaged processing operations, an assessment of the necessity and proportionality, an assessment of the risks to the rights of natural persons and the measures envisaged to address them. One of the most problematic issues in relation to this requirement is the concept of "high risk"; while the Regulation does provide several examples of operations that pose a "high risk" (systematic monitoring of publicly accessible areas on a large scale, processing special categories of data and so on),[52] data protection supervisory authorities have the power to designate other operations as being "high-risk".[53] In certain cases, controllers will have to undergo a prior consultation with the data protection supervisory authority.[54]

- **Data protection officers.** Currently, the LLPPD allows (but does not oblige) companies to appoint a representative to be responsible for data protection, who, inter alia, ensures that the company processes personal data in compliance with statutory data protection provisions.[55] Under the Regulation, businesses in most cases have discretion whether to appoint such a person, but it is mandatory to appoint a data protection officer in two cases:[56]

  1. the core activities of the company consist of processing operations which require regular and systematic monitoring of data subjects on a large scale;
  2. the core activities of the company consist of processing on a large scale of special categories of data (race, sexual orientation, genetic information and others) or personal data relating to criminal convictions and offences.

  The Regulation requires that companies involve the data protection officer in all issues relating to personal data protection and give the officer special status within the company, ensuring that he or she operates independently, reports to the highest level of management and cannot be dismissed or penalized for performing his or her tasks.[57]

- **Codes of conduct and certification.** The Regulation encourages sectoral business associations to draw up codes of conduct intended to contribute to the proper application of this Regulation, explaining its provisions in light of the particular needs of specific sectors (e.g. telecommunication companies, SMEs, cloud computing service providers). These codes should be approved by supervisory authorities,[58] with compliance being monitored by an independent third party.[59] Codes of conduct could potentially be very useful for businesses, since they would not only explain the streamlined provisions of the Regulation and provide companies with a competitive advantage in the market, but could also be seen as evidence of the controller's by compliance with the Regulation.[60] The certification mechanisms under the Regulation would operate of similar principles.[61]

While complying with the accountability principle may at times seem like "mission impossible", it is worth remembering that the Regulation does not say that the aforementioned measures are required in each and every case. Indeed, the Regulation clearly states that "[t]aking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures."[62]

As such, before selecting appropriate measures businesses would be wise to conduct an internal audit of processing procedures to identify those operations that pose the highest risk and to establish mechanisms for managing it. In addition to the measures already discussed, this could include introducing a data protection policy, training employees and so on.

52 Art. 35(3) of the Regulation
53 Art. 35(4) of the Regulation
54 Art. 36 of the Regulation
55 Art. 32 of LLPPD
56 Art. 37(1) of the Regulation
57 Art. 38(1) and (3) of the Regulation
58 Art. 40(5) of the Regulation
59 Art. 41 of the Regulation
60 „To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller." (Para. 81 of the Preamble to the Regulation)
61 Art. 42 of the Regulation
62 Art. 24(1) of the Regulation

Reducing administrative burdens

The Regulation substantially reduces the administrative burden on businesses by doing away with the current requirement under the LLPPD to register with the SDPI prior to processing personal data.[63]

The Regulation also makes it easier for businesses that are active in multiple EU states. The current regime under the Data Protection Directive required these business entities to communicate with the supervisory authorities of both states, which are often had different requirements for identical processing operations.

Since the Regulation partially harmonizes these requirements (as was mentioned before, Member States retain discretion to set their own requirements in certain fields, such data protection in employment relationships), they become easier to implement. The Regulation also introduces the concept of a "lead supervisory authority", which is of particular importance to businesses operating in multiple EU states. It means that cross-border data processing and disputes relating to such processing in practice will be the purview of the supervisory authority of the main establishment of the company.

For example, a company established in Lithuania that sells to Latvia and Estonia and consequently processes customer data will only need to "communicate" with the SDPI as opposed to three data protection inspectorates.[64] If a data subject submits a complaint to, say, the Latvian supervisory authority, it should transmit the complaint to the Lithuanian SDPI.[65] To ensure conformity in the interpretation and application of data protection rules, the Regulation provides for a consistency mechanism, which also covers disputes between the supervisory authorities of different Member States.[66]

Taking into account the special circumstances of SMEs (that is, companies with fewer than 250 employees), the Regulation allows such companies to deviate from certain data protection requirements. For example, they are not subject to the requirement to keep records of processing activities.[67] Furthermore, the Regulation urges supervisory authorities to "consider" the special needs of such companies and asks the European Commission to consider special measures for these companies.[68]

63 Art. 31 of LLPPD

64 Art. 56(6) of the Regulation. This provision does not apply if the controller is obliged to process personal data under national law or if the controller is exercising official authority (Art. 55(2) of the Regulation)

65 If the subject matter of the dispute relates only to an establishment in its Member State or substantially affects data subjects only in its Member State, the supervisory authority of that state may request its wish to handle a complaint lodged (Art. 56(2) of the Regulation). The final decision on the handling of the complaint falls to the lead supervisory authority (Art. 56(3)-(5) of the Regulation)

66 Art. 63-67 of the Regulation

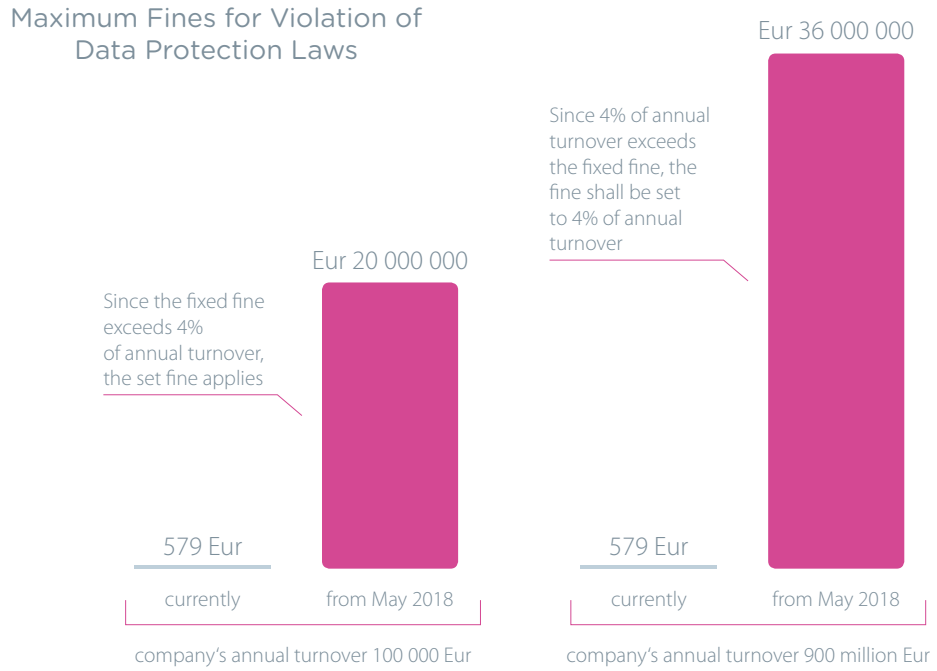
67 This exception does not apply if the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences (Art. 30(5) of the Regulation)

68 Para. 13 and 167 of the Preamble to the Regulation

Consequences of data breach

> Currently, fines for data breaches vary significantly between EU Member states. To compare, the maximum fine is just over €12,000 in Romania and Slovenia, but it can reach up to €332,000 in Slovakia and half a million Euros in the UK.[69] For instance, in 2016, the UK data protection authority fined an HIV clinic that leaked 781 patient e-mail addresses in the course of e-mail correspondence £180,000.[70]

The Regulation lays down very harsh fines for breaches, which can reach up to €20 million Euros or up to 4% of the company's total worldwide annual turnover of the preceding financial year, whichever is higher.[71] Of course, such fines are reserved for exceptionally serious, intentional violations, but it marks a stark contrast to the current regime in Lithuania (see the section titled "The current regulatory regime governing the protection of personal data in Lithuania").[72] The Regulation does not set a minimum fine, leaving that to the Member States.



69 EU Fundamental Rights Agency, „Access to data protection remedies in EU Member States", 2013, p. 21, http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en.pdf

70 Matt Burgess, „London HIV clinic fined £180,000 for 'serious' data breach", *Wired.co.uk*, 9 May 2016, http://www.wired.co.uk/article/56-dean-street-fine-data-protection-hiv

71 Art. 83(5) of the Regulation

72 For the sake of accuracy, we should note Art. 82 of the Code of Administrative Offences, which shall come into force on 1 January 2017, provides that personal data security breaches may be subject to fines up to €3,000. Code of Administrative Offences, 25 June 2015, No. XII-1869, https://www.e-tar.lt/portal/lt/legalAct/4ebe66c0262311e5bf92d6af3f6a2e8b/lJpyIHVrJb

The preparedness of Lithuanian businesses to implement the Regulation

The survey of business entities operating in Lithuania was carried by "Spinter Tyrimai", a company specializing in opinion polling and market research, and was commissioned by the Human Rights Monitoring Institute. The survey was conducted from 11 to 26 July, 2016, and took place throughout the whole of Lithuania. Representatives of 50 companies operating in Lithuania were surveyed. Respondents were selected using quota sampling, by setting quotas for different types of business entity. The three categories were startups, telecommunication and financial companies, and other, with the ratio set at 60-20-20, respectively.

Opinion on the existing regulatory regime governing data protection

Lithuania has been regulating personal data by law since 1996. At the moment, the regime is expansive, in some respects being one of the most comprehensive and strict regimes in the EU. On the other hand, Lithuania has some of the smallest fines for personal data breaches in the Union.

74% of surveyed businesses believed that the existing regulatory regime governing personal data in Lithuania was sufficient (Fig. 1).

Telecommunications and financial services companies were the most likely to find the Lithuanian regulatory regime was sufficient (80%), with companies categorized as "other" being the least likely to do so (60%). The difference is statistically significant. At present, telecommunications and financial services companies are subject to some of the highest levels of supervision, and as such can favorably look on the current regulatory regime as the established practice.

Only a slightly higher percentage of registered controllers believe that the Lithuanian regime is sufficient (78.6%), compared to unregistered controllers (72.2%). The difference is not significant and demonstrates the common need for regulatory stability.

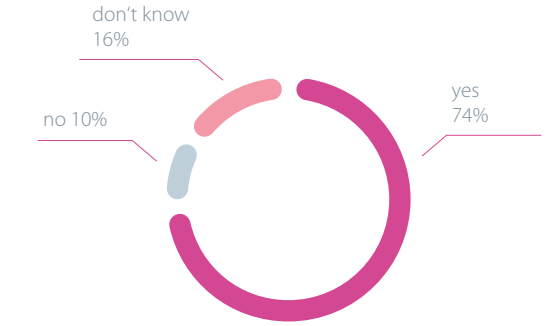


Fig. 1 Do you believe the current regulatory regime governing data protection in Lithuania to be sufficient?

Almost half of all respondents (48%) did not have on opinion on whether the fines set out in Lithuanian legislation for data breaches were currently sufficient. The other half (46%) believed that the fines were sufficient, with only a tiny minority claiming that they were not (Fig. 2).

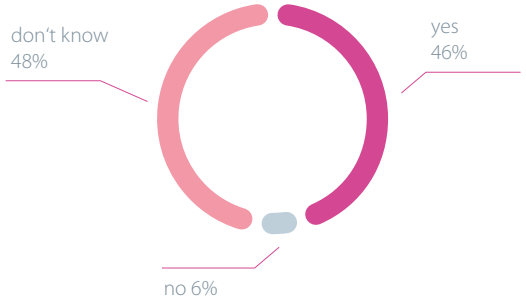


Fig. 2 In your opinion, are the current sanctions for data breaches under Lithuanian law adequate?

As we've mentioned before, Lithuania has some of the smallest fines for personal data breaches in the Union; however, they are issued fairly frequently and for minor breaches, (e.g. for not registering as a controller of personal data, when the General Personal Data Protection Regulation dispenses with the requirement entirely).

Companies in the "other" category were least aware of the fines (70%), while start-ups were the most likely to think that the fines were sufficient (53.3%). 55.6% of companies that did not register as controllers had no opinion or were not aware of the fines for data breaches, whereas among respondents from registered controllers that number was only 28,6%.

These results can be explained by the fact that registration as a controller is one of the main administrative and bureaucratic obligations for personal data controllers under the current Law on Legal Protection of Personal Data of the Republic of Lithuania. The State Data Protection Inspectorate (SDPI) fairly frequently issues mandatory instructions or sanctions for not complying with it. As a result, companies that have registered as controllers have had closer brushes with possible sanctions for data breaches. The position of startups can be explained by the fact that for startups, any sanction is a blow to the company's reputation and disrupts its activities. Presumably, this is an indication for the differentiation of sanctions in the future, with starting businesses that have little in the way of resources being subjected to more lenient sanctions, since the scale of data breaches in these companies is generally lower.

It is heartening that the majority (74%) of those surveyed trusted the institutions that are responsible supervising privacy and data protection in Lithuania, with 12% expressing full confidence and 62% being somewhat trusting (Fig. 3).

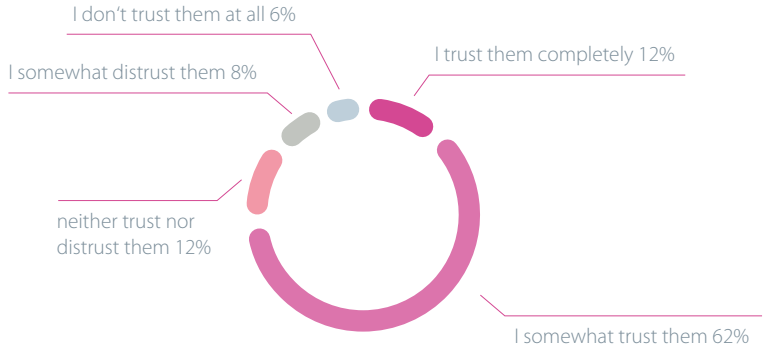


Fig. 3 Do you trust the institutions that are responsible supervising privacy and data protection in Lithuania?

Telecommunications and financial services companies were the most likely to trust Lithuanian authorities, with a whopping 80% indicating that they were somewhat trusting of them; however, nobody among them was willing to trust the authorities completely. Companies in the "other" category were the most mistrustful, at 30%. The percentage of companies trusting the authorities was almost the same for registered and unregistered controllers, standing at 78.5% and 72.2%, respectively. It is interesting to note that there were more companies that completely trusted the authorities among unregistered controllers (13.9%) than among registered ones institutions (7.1%). However, the difference here is not statistically significant.

These figures indicate that, overall, the work of the SDPI is seen in a positive light, but at the same time show that there are still shortcomings. To retain business confidence when implementing the Regulation, the SDPI should continue to exercise restraint and maintain consistency in its work, especially considering that international companies will be able to work out issues pertaining to the implementation of the Regulation with the supervisory authorities of other EU states.

The majority of the companies surveyed (72%) actually viewed data protection as very important, with 22% seeing it as moderately important and 6% considering it to be of little importance (Fig. 4). Startups boasted the highest percentage of businesses that viewed data protection as very important, as much as 76.7%, with companies in the "other" category trailing behind slightly (70%) and telecommunications and financial services companies boasting the lowest percentage (60%) of those viewing data protection as important. However, there were also no telecommunications and financial services companies that that placed no importance on data protection (see Fig. 5). Furthermore, there were no such businesses among registered controllers, with all companies that thought little of data protection being firmly in the unregistered camp.

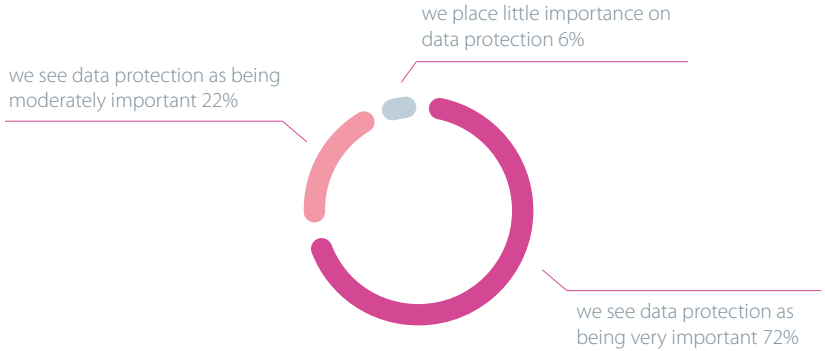


Fig. 4 How much importance does your company actually place on data protection at this time?

How much importance does your company actually place on data protection at this time?

	Startups	Telecommunications and financial services companies	Other
We see data protection as being very important	23	6	7
We see data protection as being moderately important	6	4	1
We place little importance on data protection	1	0	2

Fig. 5 How much importance does your company actually place on data protection at this time? (by company profile)

These results are encouraging and demonstrate that Lithuanian businesses are aware and responsible when it comes to processing personal data. The responses received from startups were particularly heartening. Startups very frequently have to process personal data in their work, and as such it is very important that these companies understand how crucial it is to protect personal data – in fact, this understanding may well be more important than external personal data protection rules.

Processing practices

Almost all of the surveyed companies processed data about their employees (96%) and customers (consumers) (98%), less than half of all companies processed data on their business partners (42%) and only 2% processed data on other persons. The nature of the processing varied according to the type of personal data in question. Almost all companies collected and stored data about their employees and customers (consumers). However, only 36% of companies analyzed data about their employees, while more than half (56%) analyzed data on their customers (consumers).

These types of data can also be differentiated by how many companies transmit them to others: only 4% of companies transmit data about their employees, while as much as four times more (16%) transmit data on their customers (consumers). Of those companies that processed data on their business partners, the largest percentage collected them (38%), slightly fewer stored them (28%) and analyzed them (24%), with those that would transmit such data to others being the fewest in number (8%) (see Fig. 6).

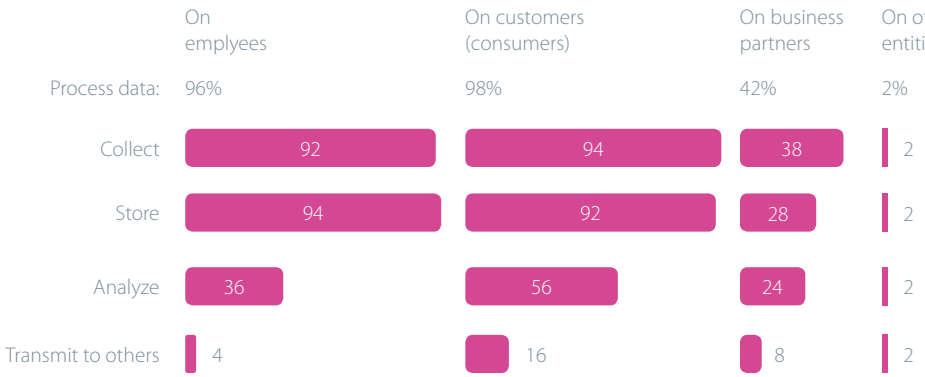


Fig. 6 What personal data does your company process and how?

The two main categories of personal data processed by Lithuanian businesses are fully in line with international practices, showing maturity on the part of companies and demonstrating their strategic orientation. That being said, the responses also show a lack of consistency when processing personal data, since most companies using video surveillance are actually processing others' personal data, with video surveillance being an exceptionally popular means of protecting life and property. Taking into account the results of the study, it is necessary to draw corporate attention to the risks posed by video surveillance and the need to protect the rights of all persons that enter the field of surveillance.

Even more surprising were the differences in responses concerning processing operations. Collecting data is essentially meaningless without storing and analyzing it. This indicates that companies do not clearly understand the concept of processing and perceive their actions in formalistic terms.

E-mail was the most popular means of processing (collection, storage, transfer) personal data (84%). 78% used information systems on company servers, 66% used cloud storage (Dropbox, Google Drive, etc.) and 32% used mobile devices that could connect to the company's IT systems (Fig. 7).

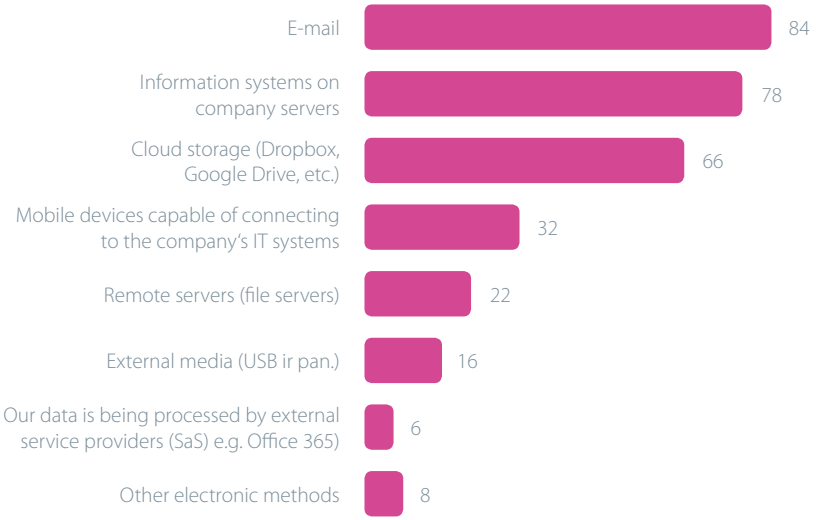


Fig. 7 Which of the following does your company use to process (collect, store, transmit) personal data?

Both startups and telecommunications and financial services companies relied mainly on e-mail, cloud storage and information systems on company servers. For companies categorized as "other", the most popular methods of processing differed, with most preferring information systems on company servers, e-mail and external media (see Fig. 8).

	Startups	Telecommunications, financial services companies	Other
E-mail	27	10	5
Cloud storage (Dropbox, Google Drive et al.)	22	9	2
Information systems on company servers	25	8	6
Remote storage (file servers)	9	0	2
External media (USB, etc.)	4	0	4
Mobile devices	12	1	3
Our data is being processed by external service providers (SaS) (e.g., Office 365)	2	0	1
Other electronic methods	3	0	1

Fig. 8 Which of the following ways your company handles (collect, store and forward) personal data? (by company profile)

These results show that Lithuanian businesses are particularly keen on using of cyber tools for processing personal data. This is a cause for concern, since companies have less control over these tools, they are continuously connected to public data networks and the data breaches that they are associated with are usually massive in scale and exceptionally harmful (for example, compromising e-mail or cloud storage security leads to a simultaneous loss of vast swathes of personal data, which threatens the security of all employees and clients). One of the objectives of the General Data Protection Regulation is to update personal data protection rules to be able to meet the challenges in cyberspace. It is likely that this could be one of the most important personal data protection topics to Lithuanian businesses.

Companies usually solve problems relating to data protection through internal means: the greatest number of respondents said that these problems are left to a member of HR/ administrative (86%), 44% had a member of IT staff take care of it, 40% had appointed an employee to take care of data protection (Fig. 9).

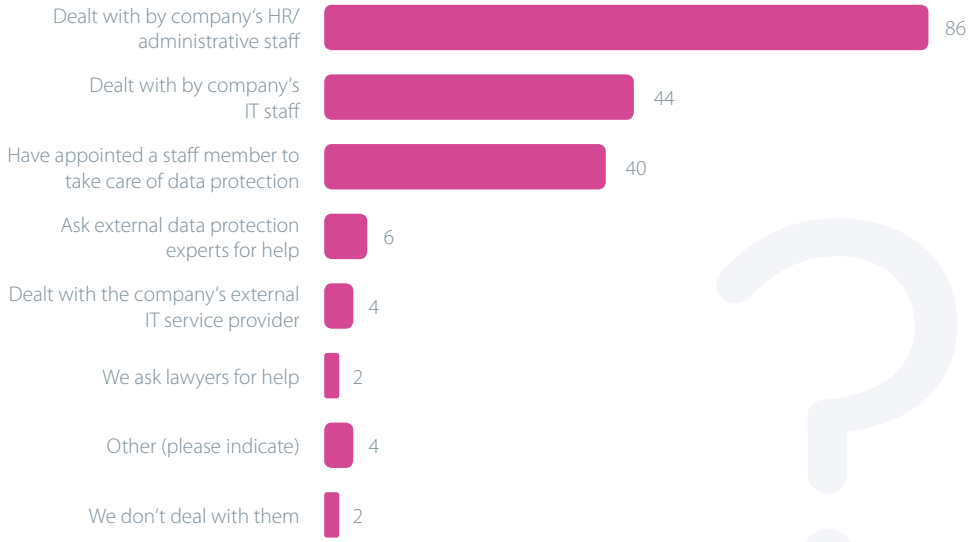


Fig. 9 How does your company deal with personal data protection issues?

Very few companies to seek assistance from external experts, namely, data protection specialists (6%), IT service providers (4%) or lawyers (2%). All telecommunications and financial services companies (100%) had HR/administrative staff members deal with data protection issues, with 50% of them having appointed an employee for this purpose, whereas IT staff members handle these issues in 40% of companies. These companies do not seek help from external experts. The situation is similar with startups and companies categorized as "other", but there were a couple of respondents among them that admitted to seeking help from external experts. One company among those categorized as "other" indicated that it does not deal with data protection issues at all; there were no such enterprises among startups and telecommunications and financial services companies.

The majority of respondents (74%) did not provide employee training on data protection issues (or did not allocate any funds towards it). Of the 26% that did offer training, 22% held training at least once a year and 4% held it less than once a year (Fig. 10).

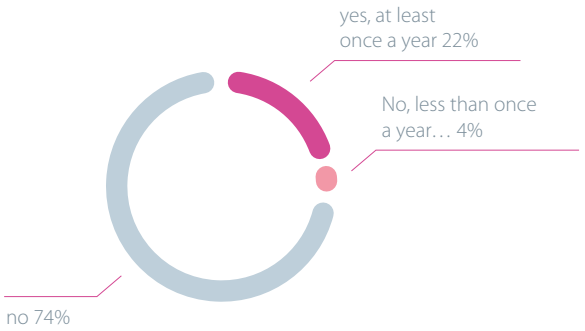


Fig. 10 Does your company provide (or allocate any funds towards) training for employees on data protection issues?

80% of startups and telecommunications and financial services companies as well as 50% of companies categorized as "other" did not offer training on data protection issues. There was a greater percentage of respondents that did not offer training among registered controllers (78.6%) than among unregistered ones (72.2%).

These results are even more worrying since they confirm our earlier observation that companies do not fully understand the risks to personal data in cyberspace. Companies rely too much on internal resources, do not consult experts and do not invest in training. Furthermore, companies that register as personal data controllers believe that they have fulfilled the formal requirements for data protection. As mentioned previously, the Regulation in general does away with administrative registration for most personal data controllers, which means that companies will interact with data protection experts even less frequently. With reference to the results of the survey, companies need to be given more information about the risks relating to the protection of personal data, promoting and supporting company consultations with experts as well as training for company employees on personal data protection issues.

Awareness of the General Data Protection Regulation

The majority (78%) of the respondents were aware of the EU General Data Protection Regulation (Fig. 11) – however, before we get ahead of ourselves, we should mention that while 70% of companies have heard about the Regulation, they were not aware of any changes it brought. Only 8% claimed knowledge of the new things being introduced. None among the telecommunications and financial services companies were aware of the coming changes. 10% of startups and an equal percentage of companies categorized as "other" were aware of the changes. Awareness of the Regulation ranked higher in the registered controller camp (85.7%) than among unregistered companies (75%).

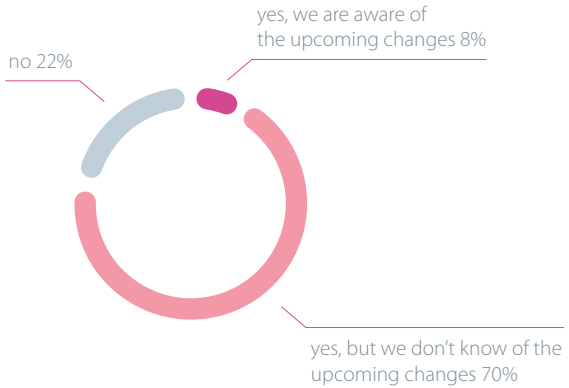


Fig. 11 Are you aware of the EU General Data Protection Regulation?

These results, together with more specific questions about how aware Lithuanian businesses are of the Regulation, show that awareness is very poor. Comprehensive measures are needed to introduce the changes brought about by the Regulation and explaining personal data protection risks in cyberspace.

82% of the companies surveyed thought that the Regulation will apply to all businesses that offer goods and services to consumers (Fig. 12) – this is the opinion of 100% of telecommunications and financial services companies, 93% of startups, but only 30% of companies categorized as "other". A whopping 50% of companies categorized as "other" do not know which companies will be subjected to the Regulation. 100% of registered controllers believe that the Regulation will apply to all businesses that offer goods and services to consumers. Among unregistered businesses, this belief is held by 75% of respondents. Moreover, 16.7% of these enterprises do not know which companies will be subjected to the Regulation, whereas no respondents among the registered controllers claimed that.

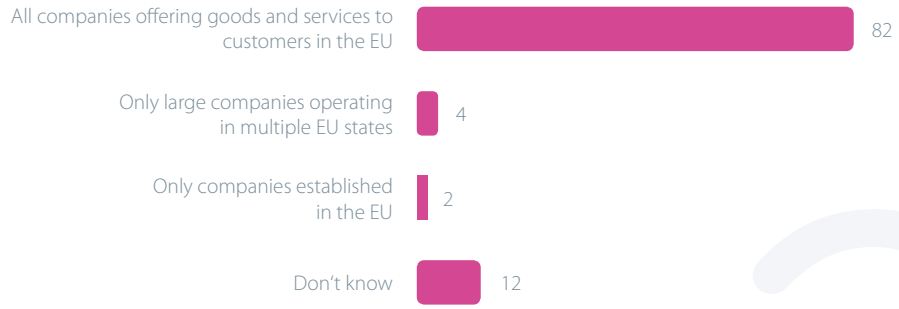


Fig. 12 Who will the General Data Protection Regulation apply to?

Most businesses intuitively understood the scope of the Regulation. However, it should be noted that issue regarding the application of the Regulation to non-EU subjects has yet to be resolved. Implementing the Regulation with respect to entities that have not been established in the EU, but offering their goods and services to EU consumers (i.e. that can simply be accessed by EU consumers online, such as Aliexpress and Snapchat), will actually be very problematic and may lead to competition problems for Lithuanian businesses when they are forced to compete with all entities operating in cyberspace on a global scale.

None of the respondents in the study were aware of the penalties for infringement under the Regulation. Bearing in mind that penalties under the Regulation are far more severe than those under the current regime in Lithuania, and knowing that this is one of the most memorable changes brought about by the Regulation, it becomes clear that companies are not familiar with the content of the Regulation, and as such businesses must be introduced to the changes brought about by the Regulation with great care.

84% of all surveyed companies have not heard about the principle of privacy by design, which applies when engineering products that use personal data. 16% had heard of this principle, with 10% choosing not to apply it in their practice and only 6% doing so (Fig. 13). None of the respondents among the "other" companies had heard of the principle of privacy by design, with 83% of startups and 70% of telecommunications and financial services companies claiming the same lack of knowledge. Only 3 startups applied the principle of privacy by design in their activities. The proportion of respondents who have not heard of this principle was higher among companies that have not registered as data controllers (88.9%) than among those that did (71.4%). Two-thirds of the companies that apply this principle in practice have been registered as personal data controllers in the SDPI database.

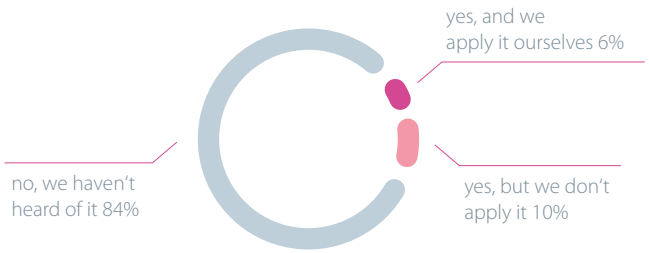


Fig. 13 Have you ever heard of the principle of privacy by design, which applies when developing products that use personal data?

These results show that Lithuanian companies maintain a formalistic approach to personal data protection, more concerned with satisfying bureaucratic and administrative requirements instead of actually protecting personal data. It is disheartening to realize that businesses do not even know what the principle of privacy by design is. This also shows that there are gaps in the education about personal data protection and that it is inadequate.

80% of respondents had not heard about data protection impact assessments. Only 20 percent had heard of these assessments, with 10% not conducting them and only 6% conducting them within their company. (Fig. 14). Only 3 companies out of all of those surveyed, two startups and one company categorized as "other", conduct data protection impact assessments surveyed. 2 of them are registered controllers and one is unregistered. In fact, the proportion of respondents that who not heard about data protection impact assessments was higher among the unregistered camp (83.3%) than among registered companies (71.4%).

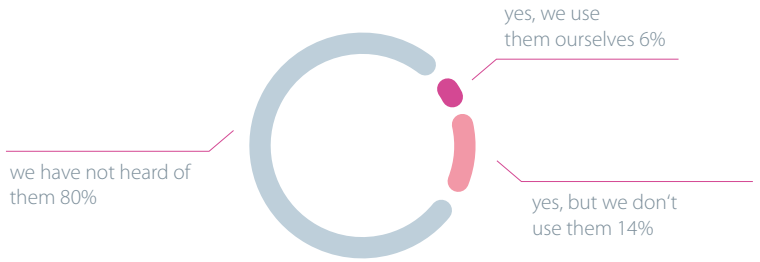


Fig. 14 Have you ever heard of data protection impact assessments?

These results confirm that Lithuanian companies hold a formalistic approach towards personal data protection and provide evidence that there are gaps in the education about personal data protection and that it is inadequate. It is clear that companies that come into contact with data protection experts are more responsible when it comes to protecting data and are more aware of current developments in the field, which confirms that experts and education are necessary. It is encouraging to know that startups are relatively more aware of modern data protection measures and make use of them. Data protection impact assessments are one of the most important new things introduced by the Regulation, affecting a majority of of businesses. Thus, to summarize, Lithuanian businesses can look forward to significant rapid changes in relation to data protection rules.

Preparedness to apply the General Data Protection Regulation

Despite the fact that only 8% of respondents claimed awareness of the changes brought about by the Regulation, no less than 60% think that their administrative burden (obligations in relation to personal data protection) will increase when the Regulation enters into force. 40% believe that that the administrative burden will not change (Fig. 15).

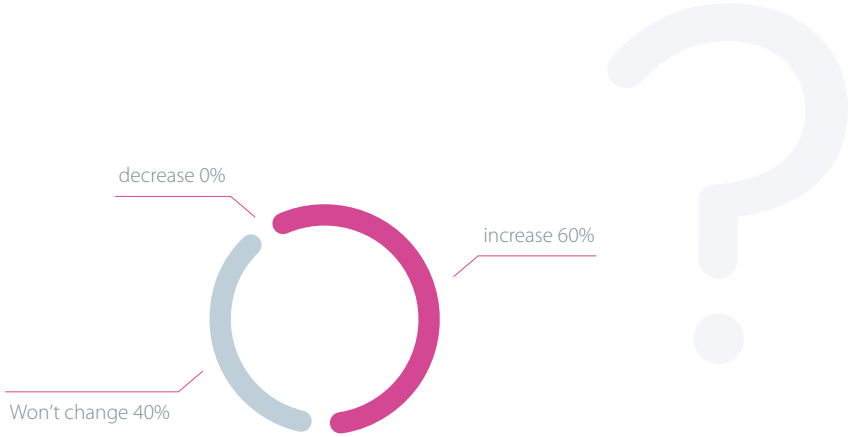


Fig. 15 How do you think the administrative burden for your company (obligations in relation to personal data protection) will change when the Regulation enters into force?

No less than 70% telecommunications and financial services companies believe that their administrative burden will increase. This is also the belief of 60% of startups and 50% of companies categorized as "other". A whopping 85.7% of companies that are registered as controllers feel that their administrative burden will increase, compared to only 50% of unregistered controllers.

These results show that, in general, companies associate regulation of personal data with increased administrative burdens. It poses a challenge to supervisory authorities, who must be able to explain the reasons behind this Regulation in particular and the legal regulation of personal data in general as well as demonstrate their advantages.

Only 26% of all respondents believed that the Regulation is more likely to have a positive impact on their company's work than not (Fig. 16). The percentage of respondents that thought that the Regulation will affect them negatively or is more likely to affect them negatively was relatively higher in the startup camp (33.3%) than among the other groups (20% of telecommunications and financial services companies and 30% of companies categorized as "other"). The group consisting of companies categorized as "other" had the lowest percentage of respondents who thought that the Regulation will affect them positively (10%). There were relatively more unregistered controllers that expected a negative outcome from the Regulation (36.1%) than registered controllers who thought the same (14.3%). The percentage of respondents that believed the Regulation will not affect them was nearly the same in both the registered and unregistered camps (42.9% and 44.4% respectively).

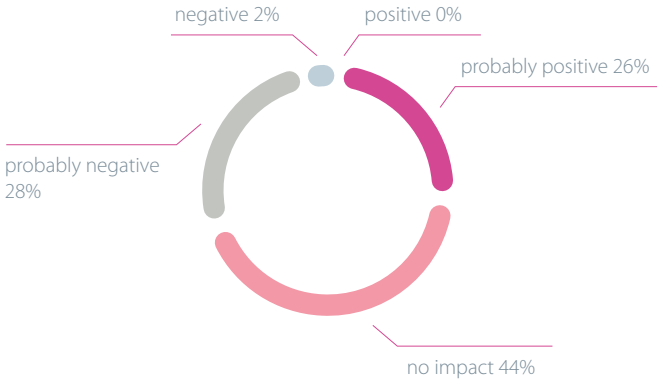


Fig. 16 How do you think the Regulation will affect the work of your company?

These responses support the notion that companies see the regulation of personal data as being related to increased administrative burdens. The regulation contains a large number rules meant to facilitate company operations, which are of particular interest to companies that do not have processing as their primary activity. Furthermore, businesses operating in multiple EU states will be able to interact with several supervisory authorities and make use of certification systems, which will likely make data protection more flexible and encourage sharing good practices between EU states. These aspects must be highlighted when talking to businesses.

The aspects of the Regulation that respondents were generally most concerned with were a drop in customer trust and loyalty (46%) and the cost of technical security measures (46%). 28% were worried about earning negative reputation due to possible security breaches, 24% were concerned with the requirement to conduct data protection impact assessments and 22% were apprehensive about potential fines (Fig. 17). It should be noted that different types of businesses were concerned with different aspects of the Regulation. For example, startups were most concerned with the cost of technical security measures (60%), companies categorized as "other" were most worried about not being able to process information to suit their business needs (being unable to carry out planned business development) and a whopping 80% of telecommunications and financial services companies were most concerned about potential fines. Among registered controllers, the most pressing concern was the fear of losing customer trust and loyalty (57.1%), while unregistered companies were most concerned with the cost of technical security measures (55.6%).

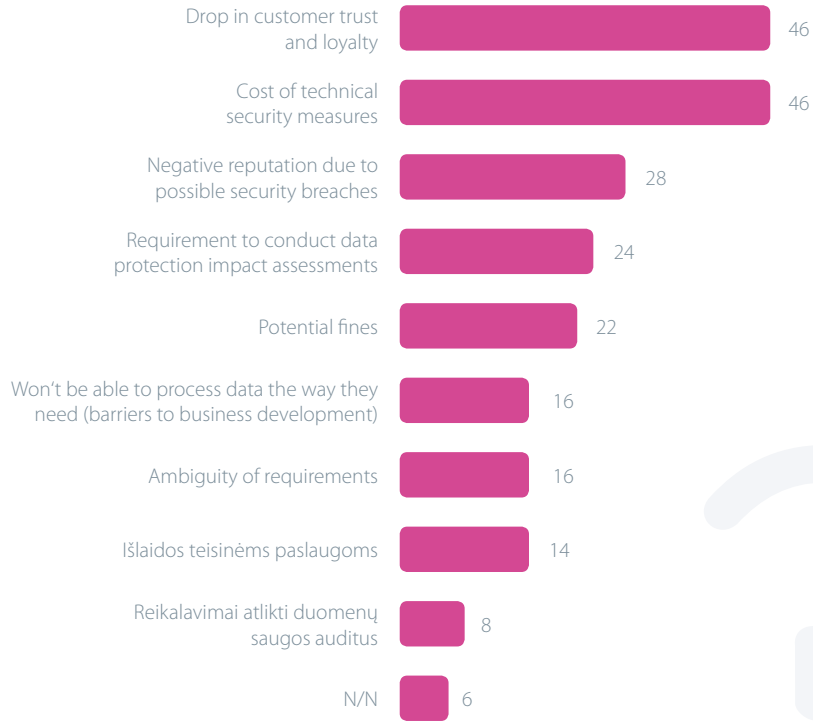


Fig. 17 What aspects of the Regulation are you most concerned about?

These results are difficult to interpret since they do not correspond to other responses. Unaware of how the regulatory regime will change, companies are worried about different things. As such, these responses should be seen not as a reflection of the expected impact of the Regulation, but rather as a reflection of the general negative expectations of companies in relation to personal data protection. Business expectations are clearly linked to the growing understanding of the threats to personal data safety, but they're also linked to the understanding that companies must invest in technical data protection measures.

Startups' concern with technical security measures can be explained by the fact that these companies have the most experience with these measures and their associated costs, which in many cases are ongoing (not one-offs) and very significant. It is clear that all companies realize that they cannot avoid investing in greater personal data security, since data security has become a common precondition to customer trust and loyalty.

Respondents are almost evenly split between those that are planning to spend on data protection over the next two years (48%) and those that are not (52%). 30% of respondents intend to spend up to €500 while 18% intend to spend between €501 to €2000 (Fig. 18). A whopping 60% startups do not plan to spend anything on data protection, whereas only 40% of telecommunications and financial services companies and the same percentage of companies categorized as "other" think the same.

Telecommunications and financial services companies are planning to spend the most, with 40% believing that they will spend between €501 and €2000 over the next two years. Only 13.3% of startups and 10% of companies categorized as "other" plan to spend the same. A greater percentage of unregistered controllers are planning on not spending anything (58.3%), compared to the registered camp (35.7%). The ranks of companies registered as controllers hold a greater percentage of respondents (42,9%) expecting to spend greater sums (€501-2000) than the ranks of the unregistered (only 8.3%).

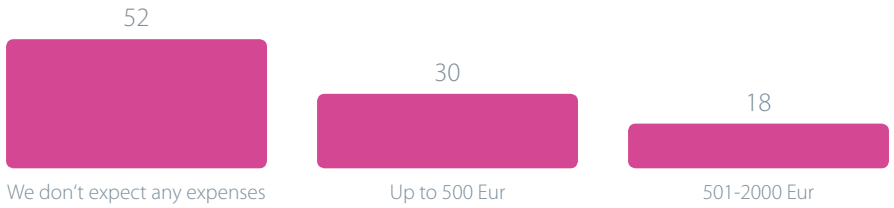


Fig. 18 What are your company's expected expenses in relation to data protection over the next two years?

Presumably, the results in this case show that companies are not aware of the requirements set out by the Regulation and therefore have not yet understood the need to invest in data security and obtain expertise in personal data matters.

Of those that believe that they will incur costs, most are planning to invest in acquiring or updating encryption technologies (75%) as well as acquiring or updating data analysis and processing technologies (70.8%) (Fig. 19). Spending priorities differ by type of company: most telecommunications and financial services companies and startups are planning to allocate funds towards acquiring or updating encryption technologies (100% and 83.3% of each group, respectively), while most companies categorized as "other" are planning to allocate funds to the maintenance of mobile devices (83.3%).

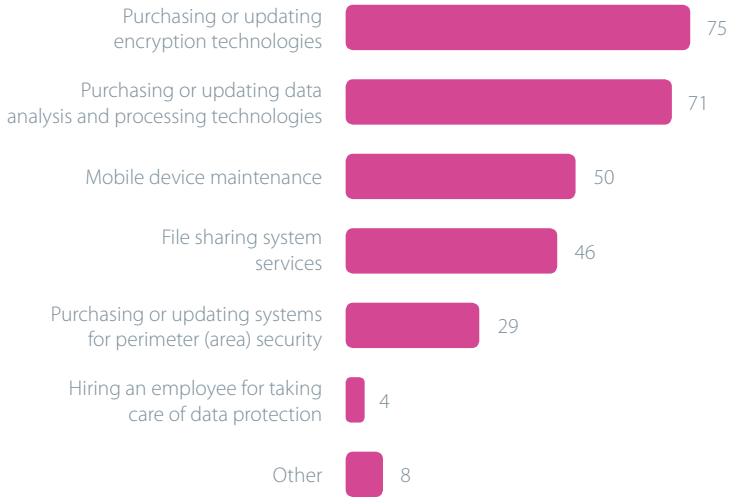


Fig. 19 How do you plan to allocate funds? (N = 24)

These results support our previous findings that most companies see personal data protection as a matter of formality. Companies are not planning to spend on training and expert advice, even though it is these areas that show the biggest gaps in the run-up to the implementation of the Regulation in Lithuania. The vast majority of companies believe that it is most important to invest in improved personal data security and focus their funding in this area. The position adopted by businesses may be explained by another question posed by this survey, the responses to which indicate that companies are expecting an active public awareness campaign about the changes brought by the Regulation.

In the run-up to the implementation of the Regulation in Lithuania, most companies would like more information on the changes brought about by Regulation (98%.) and detailed advice on satisfying its requirements (94%) (Fig. 20). According to 80% of respondents, what would be most useful is help on technological solutions required by the Regulation. There are no major differences in between startups and telecommunications and financial services companies in terms of what help is needed: both groups place equal importance on the above three aspects (between 90% and 100% of respondents). Companies categorized as "other" see technological solutions required by the Regulation as less important (30%) than startups (90%) or telecommunications and financial services companies (100%). There were no significant differences in terms of whether companies were registered controllers or not.

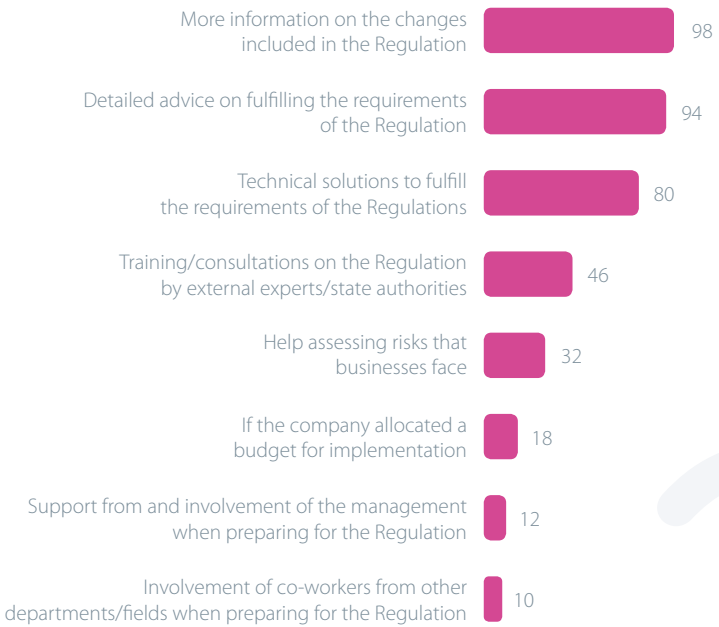


Fig. 20 What would help you to prepare for the Regulation?

These responses from companies underscore the importance of raising awareness of Regulation and draw some guidelines. When introducing the changes brought about by the Regulation in Lithuania, it is necessary to adjust company focus away from its obsession with "hard" (technical) personal data protection measures. It is necessary to emphasize the so-called "soft" measures that exist alongside them and are equal to them, in particular privacy by design, data protection impact assessments, training and other informal data protection measures. It needs to be made clear to business that the human factor and inadequate "soft" measures are responsible for many (if not most) threats to data security, the result of which is that technical security either does not suffice by itself (e.g. a poor understanding of the risks lead to applying inappropriate technical protection measures) or is vulnerable.

44% of respondents believe that the implementation of the Regulation will improve personal data protection, while 56% are of the opinion that nothing will change (Fig. 21). As much as 70% of telecommunications and financial services companies believe that nothing will change, compared to 53.3% of startups and 50% of companies categorized as "other". In relative terms, the "other" company group contains the most respondents

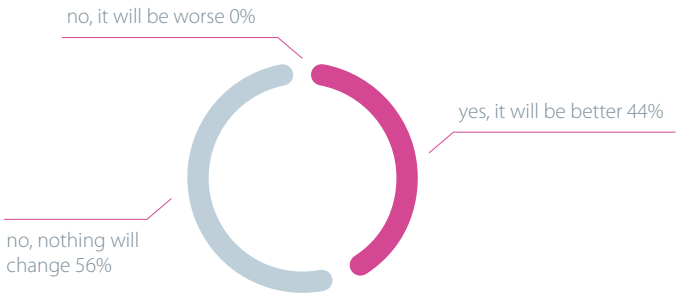


Fig. 21 In your opinion, will implementing the Regulation improve the personal data protection?

claiming that personal data protection will improve (50%); 46.7% of startups and 30% of telecommunications and financial services companies share that opinion. An equal number (50% each) among registered and unregistered data controllers believe that personal data protection will improve and not change following the implementation of the Regulation. Unregistered controllers are relatively more likely to think that personal data protection will not change (58.3%) as opposed to improving (41.7%) following the implementation of the Regulation.

Presumably, these responses are evidence of the fact that, as mentioned previously, companies do not trust the new regulatory regime. Companies are likely to link any regulation to increased administrative burdens, and as such are relatively pessimistic with respect to the implementation of the Regulation. This presents a challenge for supervisory authorities and experts. As we've mentioned before, businesses must be able to clearly see and understand the advantages offered by the Regulation in comparison to the current regulatory regime, and grasp the simplified rules.

There are still many unanswered questions regarding the implementation of the Regulation in Lithuania, including the issue of amending the Law on Legal Protection of Personal Data, reforming sanctions and the availability of expert help for SMEs when implementing the changes brought about by the Regulation.

Summary

The study clearly shows personal data protection trends and shortcomings in Lithuania. In general, we can conclude that the concept of personal data protection is not new to Lithuanian businesses. Companies understand the importance of data protection and weigh it accordingly.

However, the most prominent finding of this study is that business companies understand data protection in fairly formalistic, bureaucratic terms. It is quite likely that companies also understand personal data in narrow terms, since, despite widespread use video surveillance tools, companies do not believe that they are processing the data of unrelated people. The same could be said about the definition of processing, as companies were sharply divided on what essentially were identical processing operations.

These attitudes mostly result from inadequate education on data protection issues, seeing personal data protection as an administrative duty that provides no concrete benefits to business, as well as the current personal data protection practices of supervisory authorities. Even with the advent of new rules under the General Data Protection Regulation, most companies are planning to scrape by with "hard" (technical) data protection measures when in fact the Regulation specifically focuses on "soft" measures.

It needs to be made clear to business that the human factor and inadequate "soft" measures are responsible for many (if not most) threats to data security, the result of which is that technical security either does not suffice by itself (e.g. a poor understanding of the risks lead to applying inappropriate technical protection measures) or is vulnerable.

The second major observation made during the course is that use of new cyber technologies is widespread among Lithuanian companies. Companies rely on internal resources to manage the risks posed by these technologies, eschewing expert advice. While we must celebrate the competitive advantage brought on by cloud computing and other technologies, it is also very important to explain specific cyber security risks to businesses. These findings are also alarming in view of potential geopolitical risks.

Currently, the Regulation is still very poorly understood by Lithuanian businesses, so it is necessary to take immediate steps to increase awareness of the incoming changes. It is worth considering measure that allow companies to obtain expert advice on specific data protection issues that are of concern to the business. In all responses to the survey questions, companies that had dealings with the State Data Protection Inspectorate (companies that registered as controllers) demonstrated a greater understanding of personal data issues, which shows how important and effective company consultations are.

At present, the vast majority of companies are not aware of the advantages of the Regulation and the rules meant to facilitate company operations, which are of particular interest to companies that do not have processing as their primary activity. There is also a lack of awareness of the ability to communicate with multiple supervisory authorities in the EU and use of non-governmental data protection certification systems, which will likely make data protection more flexible and encourage sharing good practices between EU states. When teaching about the Regulation, the primary focus should rest squarely on its advantages, which will also serve to raise awareness of data protection issues.

What is most heartening is perhaps the fact that personal data protection is important to Lithuanian startups. Some apply the latest data protection practices, clearly aware of the need to constantly improve it. Presumably the administrative supervision of persons for startups, as businesses that are just getting off their feet and have little in the way of resources, could be more flexible and individualized, pertaining to their particular situation, since the scale of data breaches in these companies is generally lower.

Human Rights
Monitoring Institute