THE PRIVACY PARADOX
The Lithuanian Public’s Perceptions of Data Protection
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: Natalija Bitiukova and Karolis Liutkevičius
Peer-review: Raminta Šulskutė
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.

© Natalija Bitiukova, Karolis Liutkevičius, 2016
© Human Rights Monitoring Institute, 2016
© Indrė Vasiliauskiene (design), 2016

If you wish to receive data of this representative study 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 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.

**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.
## Content

<table>
<thead>
<tr>
<th>Definitions</th>
<th>03</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>05</td>
</tr>
<tr>
<td>Attitudes of the Lithuanian public towards data protection</td>
<td>07</td>
</tr>
<tr>
<td>Overview of EU Data protection reform</td>
<td>13</td>
</tr>
<tr>
<td>Rights of the data subject under the General Data Protection Regulation</td>
<td>16</td>
</tr>
<tr>
<td>- Consent to processing</td>
<td>17</td>
</tr>
<tr>
<td>- Right to information</td>
<td>18</td>
</tr>
<tr>
<td>- Right of access</td>
<td>20</td>
</tr>
<tr>
<td>- Right to rectification</td>
<td>21</td>
</tr>
<tr>
<td>- Right to erasure (“right to be forgotten”)</td>
<td>21</td>
</tr>
<tr>
<td>- Right to restriction of processing</td>
<td>23</td>
</tr>
<tr>
<td>- Right to data portability</td>
<td>23</td>
</tr>
<tr>
<td>- Right to object to the processing of data</td>
<td>24</td>
</tr>
<tr>
<td>- Profiling</td>
<td>24</td>
</tr>
<tr>
<td>- Remedies</td>
<td>25</td>
</tr>
<tr>
<td>Summary</td>
<td>27</td>
</tr>
</tbody>
</table>
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

Last year’s Eurobarometer showed that no less than half of all surveyed residents of Lithuania are concerned with the improper implementation of this right in practice, believing that the authorities and companies are able to use their data for purposes they were given no notice of.⁴

These fears are justified, as currently the amount of personal data being collected online is truly enormous, which, in turn, leads to corresponding levels of possible violations. Studies have shown that the most frequent data protection in the EU refer to internet-based activities, including social media, online shopping, leakage of personal data from e-shops, email account and database hacking, identity theft, security breaches and misuse of personal data by global internet companies.⁵

For a long time, the European Union sought to deal with such violations via the 1995 Data Protection Directive.⁶ However, legal professionals were quick to note that, in the context of exponential technological development, this legal instrument failed to tackle the challenges faced by digital society on a daily basis.

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.⁷ This regulation, which was adopted in April of 2016, aims to shift the balance of power between individuals and companies that process their data by granting said individuals more control over the processing.⁸

To this end, the Regulation provides for new rights, such as the right to transfer data from one service provider to another, and expands upon the existing ones, like the right to be informed about data processing and the right to request the deletion of data. Accordingly, this means stricter obligations for companies with regard to data protection, with high standards set for accountability, covering impact assessments, data protection officer appointment and notifications about data breaches. Companies that do not properly process personal data may be fined up to €20 million euro, or up to 4 % of their turnover for the fiscal year.

About the study

The study had two objectives:

1. **To assess**
   - the attitudes of the Lithuanian public towards the right to data protection

2. **To increase**
   - awareness of the right to data protection and the changes introduced by the General Data Protection Regulation

In order to assess public perceptions, we collaborated with “Spinter research” and carried out a representative survey of more than 1,000 Lithuanian residents in the July of 2016, asking questions about the right to data protection in four key areas:

- Changes to the right as a result of EU Data Protection Reform
- Violations of the right and possible remedies
- Weight given to ensuring the enjoyment of this right
- What the right entails

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.

The review of the changes brought about only covers a small (albeit crucial) part of the Regulation outlining the rights of data subjects (Chapter III). It should be noted that the present study focuses on situations where data controllers and processors are business companies, not state authorities.
Attitudes of the Lithuanian public towards data protection

The representative survey of the population was carried by “Spinter research”, a company specializing in opinion polling and market research, and was commissioned by the Human Rights Monitoring Institute. The survey was conducted from 18 to 26 July 2016 and took place throughout the whole of Lithuania. A total of 1,003 Lithuanian residents between 18 and 75 years of age were surveyed. Respondents were selected using stratified probability sampling, that is, by random selection based on targeting criteria to represent the whole of the group being studied (the population of Lithuania).

What the right to data protection entails

The Lithuanian public is not particularly knowledgeable about its rights in relation to data protection. Nearly two-thirds of respondents (65 %) admitted to being ignorant of their rights and obligations in this field. Younger respondents (between 18 and 45 years of age) and residents of major cities had a slightly better view of their knowledge, while older respondents and lower-income residents fared the worst.

Compared to the results of the surveys carried out by the State Data Protection inspectorate from 2006 to 2014, we can see that, from 2010 onwards, public awareness not only failed to grow, but has in fact declined slightly.9

9 In 2006, 2008, 2010, 2014 and 2016, the public had to answer a similar question: “Do you know your rights and obligations under the law in the field of personal data protection?” All surveys were representative. The survey was not carried out in 2012. This information was obtained from the State Data Protection Inspectorate (5 September 2016).
This poor view of one’s own knowledge is corroborated by the responses regarding the respondent’s rights in relation to data protection. Many respondents had a hard time differentiating between actual and fictional rights. On the contrary, respondents were more likely to claim rights that did not in fact exist felt than those that were provided under the law. These results show that the average data subject generally does not have a clear understanding of what he/she can demand from its data controller or processor.

<table>
<thead>
<tr>
<th>Rights provided for under the Law on Legal Protection of Personal Data</th>
<th>Percentage of the population thinking that Lithuanian laws provide for such a right</th>
<th>Rights not provided for under the Law on Legal Protection of Personal Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>To know the purpose for which data is being collected 10</td>
<td>39 %</td>
<td>To indicate which data about you is considered to be personal data</td>
</tr>
<tr>
<td>To access data about you held by the authorities or companies 11</td>
<td>19 %</td>
<td>To be able to decide in all cases whether data about you may be collected and processed</td>
</tr>
<tr>
<td>To request that unnecessary data about you be erased or destroyed 12</td>
<td>17 %</td>
<td>To control which third parties shall be able to receive data collected about you</td>
</tr>
</tbody>
</table>

In order to assess how well the right to data protection was understood, respondents were also asked to consider hypothetical situations where the right was interfered with 13 and to give an opinion on how much said interference impinged on their rights.

The responses show that the Lithuanian public is more sensitive to restrictions that have a clearer physical dimension (that is, “traditional” situations such as asking for one’s personal identification code in order to refund goods at a store or installing video surveillance cameras at the workplace without notice) were seen as the most severe violations of the right to data protection. Meanwhile, restrictions that primarily feature on the internet, such as the collection of information concerning personal browsing and social networking habits for use in personalized advertising, were seen as least interfering with the subjects’ rights.

\[\begin{array}{|l|c|}
\hline
\text{Situation} & \text{Percentage} \\
\hline
\text{Required to provide personal identity code when returning goods to the store} & 751 \\
\text{Installing video surveillance cameras in a person’s workplace without their knowledge} & 748 \\
\text{Right of law enforcement authorities to demand that telecommunications service providers give information on a person’s e-mail correspondence} & 739 \\
\text{Storing data about a person’s browsing history (which page he or she visited and for how long) at the telecommunications service provider} & 736 \\
\text{Storing data at the workplace about a person’s e-mail correspondence using a work e-mail address, to assess the quality of their work} & 715 \\
\text{Neighbour installs video surveillance cameras that catch a person’s home door in their field of view} & 705 \\
\text{Potential employers checking your publicly available Facebook (or any other social network) profile to assess your eligibility as a candidate} & 700 \\
\text{Using your browsing history and habits on Facebook to present ads tailored to your tastes} & 693 \\
\hline
\end{array}\]

In your opinion, which of these situations represent a breach of the right to data protection?

1 – no breach at all  
10 – a serious violation

\[\begin{array}{|l|}
\hline
\text{Situation} & \text{Percentage} \\
\hline
\text{Required to provide personal identity code when returning goods to the store} & 751 \\
\text{Installing video surveillance cameras in a person’s workplace without their knowledge} & 748 \\
\text{Right of law enforcement authorities to demand that telecommunications service providers give information on a person’s e-mail correspondence} & 739 \\
\text{Storing data about a person’s browsing history (which page he or she visited and for how long) at the telecommunications service provider} & 736 \\
\text{Storing data at the workplace about a person’s e-mail correspondence using a work e-mail address, to assess the quality of their work} & 715 \\
\text{Neighbour installs video surveillance cameras that catch a person’s home door in their field of view} & 705 \\
\text{Potential employers checking your publicly available Facebook (or any other social network) profile to assess your eligibility as a candidate} & 700 \\
\text{Using your browsing history and habits on Facebook to present ads tailored to your tastes} & 693 \\
\hline
\end{array}\]

Find out more

\[\begin{array}{|l|}
\hline
\text{The right to data protection under the Law on Legal Protection of Personal Data} & \\
\text{Data subjects’ rights under the General Data Protection Regulation} & \\
\hline
\end{array}\]

\[\begin{array}{|l|}
\hline
\text{DEFINITIONS} & \text{PREFACE} & \text{OVERVIEW OF EU DATA PROTECTION REFORM} & \text{SUMMARY} \\
\hline
\text{ATTITUDES OF THE LITHUANIAN PUBLIC TOWARDS DATA PROTECTION} & \text{What the right to data protection entails} & \text{The current regulatory regime governing the protection of personal data in Lithuania} & \\
\text{What the right to data protection entails} & \text{Weight given to the right to data protection} & \text{Rights of the data subject under the General Data Protection Regulation} & \\
\text{Defending the right to data protection} & \text{Awareness of the EU Data Protection Reform} & \\
\hline
\end{array}\]
Weight given to the right to data protection

More than three-quarters of respondents said that they see data protection being as important as the "classic" human rights more often encountered in public discourse, such as the right to freedom of expression or the right to a fair trial. This view was most prominent among young (18-25 years of age) respondents, respondents with university or college degrees as well as those with higher incomes – more than 80 % of the individuals of each of these groups held the right to data protection to be a full-fledged human right.

However, barely more than one in four consumers of electronic communications services pay attention to the practical implementation of this right when it comes to everyday decisions: only 29 % of all respondents always (or at least usually) read the terms and conditions regarding data processing when entering into a contract with a provider of goods or services that collects personal data. Nearly as many respondents (28 %) never take an interest in the terms of the contract. The remaining 43 % read these terms and conditions occasionally or very rarely.

In your opinion, should the right to the protection of personal data be given the same weight as a person’s right to freedom of expression or the right to a fair trial?

- **Yes** 77 %
- **No** 23 %

Do you take time to get to know the published Data Processing Rules/Privacy Policy of a supplier of goods or services (for example, a telecommunications company or an online shop)?

- **Yes, always** 7 %
- **Yes, usually** 22 %
- **Yes, occasionally** 22 %
- **No** 28 %
- **Yes, but rarely** 21 %

Find out more

However, in this instance "yes" should be treated with caution. An experiment conducted by US digital communications professors in 2015 showed that 74 % of the 543 participating students joined a new social network without first reading its privacy policy, while 26 % of those that did read it only spent 73 seconds (if we consider average reading speed, it should have taken students around half an hour). 98 % of all participants clicked "agree" without noticing that they agreed to hand over their first born child as payment for using the social network, and that the social network was obliged to share all data on the participants to their employers and the US National Security Agency.14

On the other hand, you can hardly blame the participants. Reading lengthy privacy rules is a difficult task due to both time constraints and their technical language. It is estimated that, on average, it would take internet users 244 hours each year to read through the privacy rules of each and every site they visit, which in turn is more than half the time that the average user spends online.15

This fact is also confirmed by the analysis conducted by the law firm Triniti between April-May of 2016: out of 50 Lithuanian web portals with a variety of content, only 22 explain to the users that their data shall be processed, of which only 4 do so in a clear language. Privacy policies are often penned in such a way that that even lawyers find them difficult to read and understand.16

---

16 Daugailė Syrusaitė, "More than half of companies collecting personal data online are acting unlawfully", triniti.lt, 1 August 2016, http://triniti.lt/2016/08/01/daugiau-nei-puse-asmens-duomenis-internete-renkanciu-imoniu-tai-daro-neteisetai/
Only one in five respondents said that they were resolved to take action upon finding out that their provider of goods or services has breached their right to the protection of personal data (i.e. resolved to switch to a different provider). These were mainly young (18-25 years of age) people and those with university or college degrees. A large portion of all respondents (41%) would consider the possibility (“Probably yes”), but almost as much (40%) would likely take no action (“Absolutely not”/“Probably not”).

Would you switch to a different goods or service provider (for example, a telecommunications company or an online store) if you found out that the current one has been sanctioned for the misuse of personal data?

- Yes, definitely 19%
- Yes, probably 41%
- Probably not 25%
- Definitely not 15%

Respondents were even less willing to invest in guarantees regarding their right to data protection. Only 3% were willing to pay an additional fee to their e-mail provider for maximum data protection. Meanwhile, 12 times more respondents (37%) firmly stated that they would not pay an extra fee (“Absolutely not”). The majority of respondents (60%) had no strong opinion on the issue, with those more likely to pay and those less likely to pay claiming near-equal shares (28% and 32%, respectively).

Would you be willing to pay an additional fee to your e-mail provider for maximum data protection? (data would not be shared with other companies and there would be no advertising)

- Yes, certainly 3%
- Yes, probably 28%
- Probably not 32%
- Certainly not 37%

The survey results point to something that researchers like to call “privacy paradox”17. The paradox shows the difference between opinion and behaviour: while most consumers claim to hold the right to data protection in high regard, only a minority would take active steps to implement it in practice. Researchers have identified several reasons for this paradox:

- information asymmetry – people are rarely fully aware of what information about them is held by the authorities and businesses, as well as how exactly that information is used;
- erroneous views – some consumers believe that the mere fact that a site has privacy rules in place means that its administrators would not share data with third parties;
- difficulties in understanding the damage caused by data security breaches, which is not expressed in clear financial terms and seems quite remote, especially when compared to the benefits of using ‘free’ services (e-mail, loyalty discounts, etc.) or the joy at being able to access the desired service in a couple of seconds;
- context resulting from the behaviour of others around the person, cultural and social norms pertaining to what is “acceptable” – how much and what type of information may be shared in one’s environment.18

Still, research shows that eliminating the underlying reasons of the paradox, such as information asymmetry, results in a corresponding change in people’s behaviour. For example, one experiment found that when a search engine would only allow comparing the price of goods in different online shops, buyers were not inclined to pay attention to the site’s privacy rules and opted for the lowest price. However, when the price was also accompanied by a symbol indicating the level of data protection offered (as determined by analyzing the privacy rules), the majority of buyers were willing to pay up to 5% extra for a vendor that offered better protection of their data.19

---


19 Ibid., p. 510
Defending the right to data protection

The survey also sought to assess what Lithuanian residents would do (and how active they would be) to defend their right to data protection in case of a breach. In particular, we investigated which institution people would approach to protect this right. Naturally, there is no single correct answer to this question, as which institution is the “correct” one would depend on many factors, such as which aspect of the right to privacy had been violated, who committed the violation and how it was done, the scope of the violation and the like. Therefore the responses to this question serve more to illustrate the attitudes of the respondents – that is, the nature of the violations they think they are likely to run into.

When asked what institution they would first approach if they suspected there was a breach of their right to data protection, 36% of all respondents indicated the police. As such, we can assume that violations of this right are usually associated with criminal offenses that feature personal data as one of their elements. This assumption is reinforced by the results of the 2015 Eurobarometer survey. The majority of Lithuanian residents claimed that they perceive fraud, identity theft and data usage without their knowledge as the greatest possible threat when submitting personal data electronically.20

Two other notable groups of respondents stated that they would approach the State Data Protection Inspectorate (10%) or go to court (8%) – in these cases, personal data breaches were possibly interpreted as offenses belonging to a separate, discrete category.

Still, a whopping third of all respondents could not specify an institution where they would seek redress. This shows that a large portion of the Lithuanian public does not have a clear understanding of the types of violations of the right to data protection it may come into contact with.

One in ten respondents thought to have experienced a violation of their right to data protection at some point. The vast majority (81%) took no action to remedy the breach. The two most common stated reasons for such apathy were lack of knowledge of where to go and the belief that nothing good will come of it. However, pessimism in the latter case may be somewhat exaggerated, since at least half of the small group of respondents that sought a remedy have reported being successful.

Did you take any steps to defend your right to data protection? (N=95)

<table>
<thead>
<tr>
<th>Institution</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Police</td>
<td>36</td>
</tr>
<tr>
<td>State Data Protection Inspectorate</td>
<td>10</td>
</tr>
<tr>
<td>Court</td>
<td>8</td>
</tr>
<tr>
<td>Law enforcement/lawyer</td>
<td>4</td>
</tr>
<tr>
<td>Close ones, friends, relatives</td>
<td>2</td>
</tr>
<tr>
<td>Consumer Rights Protection Authority</td>
<td>2</td>
</tr>
<tr>
<td>Prosecutor’s office</td>
<td>2</td>
</tr>
<tr>
<td>Other</td>
<td>1</td>
</tr>
<tr>
<td>N/N</td>
<td>33</td>
</tr>
</tbody>
</table>

Where would you first go in the event of a data security breach?

<table>
<thead>
<tr>
<th>Why? (N=77)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not think it would help</td>
</tr>
<tr>
<td>Did not know where to go</td>
</tr>
<tr>
<td>Other</td>
</tr>
</tbody>
</table>

Two other notable groups of respondents stated that they would approach the State Data Protection Inspectorate (10%) or go to court (8%) – in these cases, personal data breaches were possibly interpreted as offenses belonging to a separate, discrete category.

Still, a whopping third of all respondents could not specify an institution where they would seek redress. This shows that a large portion of the Lithuanian public does not have a clear understanding of the types of violations of the right to data protection it may come into contact with.

One in ten respondents thought to have experienced a violation of their right to data protection at some point. The vast majority (81%) took no action to remedy the breach. The two most common stated reasons for such apathy were lack of knowledge of where to go and the belief that nothing good will come of it. However, pessimism in the latter case may be somewhat exaggerated, since at least half of the small group of respondents that sought a remedy have reported being successful.

Find out more

New remedies under the Regulation
Awareness of the EU Data Protection Reform

As was already mentioned, the General Data Protection Regulation will be applied in the EU starting 25 May 2018 and will change the EU and Lithuanian data protection regimes in many areas. More than three-quarters of Lithuanians (78%) know next to nothing about it. Of the minority that actually have heard of this new law, only a small portion of the respondents were aware of specific planned changes – in fact, they comprised just 5% of all respondents. The latter group consisted mostly of young adults (18-25 years of age) and respondents with a university or college degree.

This may be because the Regulation is most often discussed in publications aimed at professionals (businessmen, lawyers, IT specialists), which the general public finds insufficiently clear and hard to understand.21

Have you heard that the General Data Protection Regulation will come into force at EU level in 2018, fundamentally changing the existing data protection regulations?

- I have heard of it and I am aware of the impending changes, 5%
- I have heard of it, but I’m not aware of any changes, 17%
- I have not heard of it, 78%

Only one in five respondents indicated that they will take a closer look at the changes proposed by the EU. Once again, these were mostly young adults (18-25 years of age), people with university or college degrees and higher-income respondents.

The most popular way of obtaining information on the new EU Regulation was through TV and radio broadcasts – this was the preferred method of a little over half of the respondents intending to find out more about the new regime. The internet was another prominent venue, preferred by one in four respondents.

Find out more

What will the General Data Protection Regulation bring?

OVERVIEW OF EU DATA PROTECTION REFORM
- The current regulatory regime governing the protection of personal data in Lithuania
- Rights of the data subject under the General Data Protection Regulation

DEFINITIONS

ATTITUDES OF THE LITHUANIAN PUBLIC TOWARDS DATA PROTECTION
- What the right to data protection entails
- Weight given to the right to data protection
- Defending the right to data protection
- Awareness of the EU Data Protection Reform

SUMMARY
Overview of EU Data protection reform

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. The law was later amended to transpose 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.

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. 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.

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. This could be their name, personal identification code, date of birth, fingerprints, biometric data or even their IP address. The LLPPD distinguishes special personal data from all other personal data, prohibiting its processing except for the circumstances outlined in the act. 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.

Persons whose personal data is being processed are called data subjects. 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.

22 Art. 2(1) of LLPPD
24 Art. 2(6)-(7) of LLPPD
25 Art. 1(4) of LLPPD
26 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)
27 Art. 5(2) of LLPPD
28 Art. 2(8) of LLPPD
29 In this study, “data subject,” “person” and “resident” are used interchangeably unless noted otherwise.
30 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 Elfer v. Land, C-92/09 and C-93/09, 9 November 2010, para. 52).
31
Processing is defined in very broad terms, covering any and all operations performed on personal data, such as collection, recording, organization, storage, classification, grouping, combination, alteration, disclosure, publication, use, logical or arithmetic operations, retrieval, dissemination, destruction et al.\(^{32}\)

Processing is only lawful when done based on one or more of the following criteria:\(^{33}\)

<table>
<thead>
<tr>
<th>Criteria for the lawful processing of personal data</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>The person has consented to having his data processed</td>
<td>To register at an online shop, you enter your name and e-mail on the registration form. You also tick the box &quot;I agree to receive the newsletter containing information about new products.&quot;</td>
</tr>
<tr>
<td>Processing is necessary for the performance of the contract to which data subject is a party</td>
<td>When entering into a residential lease agreement, you provide the lessor with your personal data (your name, personal identification code and others).</td>
</tr>
<tr>
<td>The controller has a legal obligation to process personal data</td>
<td>The Lithuanian Labour Code provides that employers must give notice to the state social insurance authority about the start of a person's employment. The notification contains such data as the new employee's name, personal identification code, social security number and others.(^{35})</td>
</tr>
<tr>
<td>Processing is necessary to protect vital interests of data subject</td>
<td>When a person goes missing, his name and image are made public and disseminated to aid in the search.</td>
</tr>
<tr>
<td>Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller</td>
<td>The Law on Equal Opportunities for Women and Men provides that the Office of the Equal Opportunities Ombudsperson must investigate complaints of discrimination. During the investigation, the Office processes the following data: the complainant’s name, address and, in some cases, the name of their employer and their job title.(^{36})</td>
</tr>
<tr>
<td>Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed</td>
<td>A company collects data on a debtor and submits it to court in order to recover the amount owed.</td>
</tr>
</tbody>
</table>

\(^{32}\) Art. 2(4) of LLPPD

\(^{33}\) It should be noted that the processing criteria for exceptionally sensitive (special) data is different, see Art. 5(2) of LLPPD

\(^{34}\) Art. 5 of LLPPD


\(^{36}\) Law No. VIII-947 on Equal Opportunities for Women and Men, 1 December 1998, Art. 12(1) and 19, https://www.e-tar.lt/portal/lt/legalAct/TAR.746227138BCB/QymFynrYKVU
The LLPPD sets out the requirements for processing personal data, the rules that controllers and processors must follow and the four basic rights that data subjects have:\(^{37}\)

The LLPPD also provides a mechanism for defending these rights: if data subjects believe that one or more of their rights have been violated, they may complain to the State Data Protection Inspectorate.\(^{38}\)

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.\(^{39}\) Fines for unlawfully processing of data or violating the data subject’s rights range from €144 to €579.\(^{40}\)

In addition to the Inspectorate, it is also possible to go to other institutions, including the police,\(^{41}\) the Inspector of Journalistic Ethics\(^{42}\) and the courts. The selection of available authorities depends on the nature of the breach of personal data and the person’s expectations. For example, pecuniary or non-pecuniary relief may only be granted by court. This may be done on the basis of Art. 2(23) of the Civil Code, which protects the right to privacy and secrecy.\(^{43}\)

\(^{37}\) Art. 23 of LLPPD

\(^{38}\) Art. 42 of LLPPD


\(^{40}\) Ibid.

\(^{41}\) With reference to Art. 167 of the Criminal Code, unlawful collection of information about a person’s private life is a criminal offence, with unlawful disclosure or use of information about a person’s private life being a criminal offence under Art. 168. See the Criminal Code, 26 September 2000, No. VIII-1968, https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/NkpvL.EzqCb


Rights of the data subject under the General Data Protection Regulation

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 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.\(^4^6\) 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.\(^4^7\) The Regulation will be applied from 25 May 2018, giving both Member States and businesses time to prepare for its implementation.\(^4^8\)

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 include 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.\(^4^9\)

It is estimated that the Regulation contains more than fifty such “flexible” provisions,\(^5^0\) 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 should cease to apply on 25 May 2018.

The following is an overview of the fundamental rights of data subjects under the Regulation, comparing them to their rights under the LLPPD, which were discussed above.

Consent to processing

In essence, the criteria for lawful processing set out in the Regulation are similar to those set out in the LLPPD. However, the Regulation is stricter when it comes to data being processed with the data subject’s consent. To be effective, consent must be freely given, must be specific, unambiguous and informed. If the intent is to process special personal data, consent must be explicit. In addition, companies must ensure that “it [is] as easy to withdraw as to give consent.”

For example, consent may be given by ticking the box “I agree with the Privacy Policy” on a website’s registration form, which leads to that site’s privacy regulations (Example 1). Consenting is an action, which means that pre-ticked boxes (“tacit consent”) do not constitute proper consent (Example 2).

In order for the data subject’s consent to processing to be informed, the company’s request must be expressed clearly and distinguished from all other requests, meaning that it cannot be “hidden” under the request to agree to the site’s terms and conditions (Example 3). To this end, webmasters ideally should include at least two separate boxes in their registration forms, one for the privacy policy and the other one for the general terms and conditions.

---

51 Art. 9 of the Regulation
52 Art. 4(1) of the Regulation. In addition, Art. 8 of the Regulation sets out addition requirements for obtaining a child’s consent, but they are beyond the remit of this study.
53 “Explicit consent” is distinct from “unambiguous consent” The Regulation asks for explicit consent in three cases: when processing special categories of data (Art. 9(2)(a) of the Regulation); when the decision-making process is automatic, including profiling (Art. 22(2)(c) of the Regulation); when personal data is transferred to a third party (Art. 49(1)(a) of the Regulation). For more about explicit and unambiguous consent, see Phil Lee, "The ambiguity of unambiguous consent under the GDPR", Privacylawblog.fieldfisher.com, 7 June 2016, http://privacylawblog.fieldfisher.com/2016/the-ambiguity-of-unambiguous-consent-under-the-gdpr/
54 Art. 7(3) of the Regulation.
55 The preamble to the Regulation speaks of “tacit consent”: “Silence, pre-ticked boxes or inactivity should not therefore constitute consent”
56 Art. 7(2) of the Regulation
Right to information

The principle of fair and transparent processing requires companies to provide individuals with information about how their data is being processed. When it comes to eservices, this information is usually provided in the website’s “Privacy Settings”. To ensure that individuals are able to effectively enjoy this right, the information should be provided in a “transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.”

Considering the length of the obligatory information, standardized icons may be used alongside the habitually long and overcomplicated privacy rules to meet this requirement (Example 4).

Below you will find a comparison between the kinds of information that controllers must provide to data subjects prior to collecting their data under the LLPPD and the Regulation.

<table>
<thead>
<tr>
<th>Law on Legal Protection of Personal Data</th>
<th>General Data Protection Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity of the controller</td>
<td>Identity and contact details of the controller</td>
</tr>
<tr>
<td>Purpose of processing</td>
<td>Purpose of and legal basis (criterion) for processing</td>
</tr>
<tr>
<td>Whom and for what purposes shall receive personal data</td>
<td>The recipients or categories of recipients of personal data</td>
</tr>
<tr>
<td>Whether the data subject is obliged to provide personal data and the possible consequences of a failure to do so</td>
<td>Whether the data subject is obliged to provide personal data and the possible consequences of a failure to do so</td>
</tr>
<tr>
<td>The data subject’s right to access his or her own data, ask for rectification or object to processing</td>
<td>The Data subject’s right to access his or her data, ask for rectification, erasure, restriction on processing, object to processing and the right to data portability</td>
</tr>
<tr>
<td>Other information necessary to ensure that personal data is processed correctly</td>
<td>The contact details of the data protection officer, if applicable</td>
</tr>
<tr>
<td></td>
<td>The legitimate interests pursued by the controller or third party (if data is being processed on these grounds)</td>
</tr>
<tr>
<td></td>
<td>The controller’s intent to transfer personal data to a recipient in a third country or international organization, with reference to the appropriate or suitable safeguards</td>
</tr>
<tr>
<td></td>
<td>The period for which the data will be stored</td>
</tr>
<tr>
<td></td>
<td>The right to withdraw consent for processing data</td>
</tr>
<tr>
<td></td>
<td>The right to lodge a complaint with a supervisory authority (in Lithuania, that’s the State Data Protection Inspectorate)</td>
</tr>
<tr>
<td></td>
<td>The existence of automated decision-making, including profiling, meaningful information about the logic involved as well as the consequences of such processing</td>
</tr>
</tbody>
</table>

Example 4

Icons for the Mozilla Firefox web browser, by designer Aza Raskin

57 Art. 5(1)(a) of the Regulation
58 Art. 12(1) of the Regulation
59 Art. 12(7) of the Regulation. In addition, Art. 12(8) of the Regulation empowers the Commission to regulate the procedures for providing standardized icons, so there may be changes in this area.
61 This information must be provided when directly collecting data from the data subject. Information that needs to be provided when obtaining data from someone other than the data subject is specified in Art. 24(2) of LLPPD and Art. 14 of the Regulation.
62 The information specified in Art. 24(1) of LLPPD need not be provided if the data subject is already in possession of it.
63 The information specified in Art. 13(1) of the Regulation need not be provided if the data subject is already in possession of it (Art. 13(4) of the Regulation).
64 Persons need to be informed of their right to object to processing only if their data is being processed for the purposes specified in Art. 5(1)(5)-(6) of LLPPD, or for direct marketing purposes.
One part of the person’s right to information that takes effect at a later stage (that is, after processing has begun) is the right to be notified of any data breaches. Hacker attacks, when third parties get a hold (or may get a hold) of data, are considered to be breaches of this sort. In Lithuania, only telecommunications companies, Internet service providers and other companies providing electronic communications services are under an obligation to notify the person of a security breach. The Regulation obliges all companies and institutions managing personal data to do the same, irrespective of the nature of their operations.

When the security breach is likely to result in a high risk to the rights and freedoms of a person, data subjects have the right to obtain such information without delay, in clear and plain language. Data subjects should be informed not only about the nature of the infringement, but also about its consequences, any measures taken by the company and the person that may be contacted regarding this issue. This right may be ensured in different ways – for example, in the event of large-scale breaches, where it is difficult to inform all data subjects individually, information regarding the breach could be given publicly (Example 5).
Right of access

The Regulation contains a repeat of the right of access already provided under the LLPPD. Both pieces of legislation provide that, upon submitting a request to the controller, persons are entitled to:

- confirmation as to whether or not data concerning them is being processed
- a copy of the data being processed
- additional information

The Regulation provides that the right to a copy of the data “shall not adversely affect the rights and freedoms of others.” To find out what these rights and freedoms are, it is wise to refer to the EU Charter of Fundamental Rights. It should be noted that the Charter provides a fairly broad list of rights and freedoms, including the freedom to conduct business and the right to the protection of intellectual property. It is likely that companies shall rely on these provisions to limit access to personal data to protect intellectual property, confidential information or trade secrets.

The additional information that must be provided upon request differs between the LLPPD and the Regulation. Below is a comparison of information categories:

<table>
<thead>
<tr>
<th>Law on Legal Protection of Personal Data</th>
<th>General Data Protection Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>What data was collected from which sources</td>
<td>Where the personal data are not collected from the data subject, any available information as to their source</td>
</tr>
<tr>
<td>The purposes of processing</td>
<td>The purposes of processing</td>
</tr>
<tr>
<td>Data recipients that have been receiving or received data in the last year</td>
<td>The recipients or categories of recipients of personal data, in particular recipients in third countries or international organizations and the appropriate safeguards relating to the transfer</td>
</tr>
<tr>
<td>The period for which the data will be stored</td>
<td>The Data subject’s right to access his or her data, ask for rectification, erasure, restriction on processing, object to processing</td>
</tr>
<tr>
<td>The right to lodge a complaint with a supervisory authority (in Lithuania, that’s the State Data Protection Inspectorate)</td>
<td>The right to lodge a complaint with a supervisory authority (in Lithuania, that’s the State Data Protection Inspectorate)</td>
</tr>
<tr>
<td>The existence of automated decision-making, including profiling, meaningful information about the logic involved as well as the consequences of such processing</td>
<td>The existence of automated decision-making, including profiling, meaningful information about the logic involved as well as the consequences of such processing</td>
</tr>
</tbody>
</table>

---

71 Art. 25 of LLPPD, Art. 15 of the Regulation
72 Art. 25(3) of the Regulation
74 Art 16 of the Charter.
75 Art 17 of the Charter.
Right to rectification

Like the LLPPD, the Regulation allows individuals to ask the controller to rectify inaccurate data.79 While the controller is checking and rectifying inaccurate information, the person may request that data concerning him or her not be rectified for the time being (see section titled “Right to restriction of processing”).

Right to erasure (“right to be forgotten”)

Although this is often presented as a new right, the LLPPD in fact also provides for the right to erasure. The latter law provides for the right to request the “destruction” of data. As such, what’s actually new is probably the fact the Regulation provides a detailed list of causes for approaching the controller to exercise this right, and sets out the procedure for doing so.

First, let us compare the circumstances in which a person may exercise this right:

<table>
<thead>
<tr>
<th>Law on Legal Protection of Personal Data</th>
<th>General Data Protection Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data is being processed unlawfully, unfairly</td>
<td>Data has been unlawfully processed</td>
</tr>
<tr>
<td></td>
<td>The data is no longer necessary in relation to the purposes for which it was processed</td>
</tr>
<tr>
<td></td>
<td>The data subject withdraws consent and there no other legal grounds for processing</td>
</tr>
<tr>
<td></td>
<td>The data subject objects to the processing and the controller can find no overriding legitimate grounds for processing (see section titled “Right to object to the processing of data”)</td>
</tr>
<tr>
<td></td>
<td>EU or national law requires that the data be erased</td>
</tr>
<tr>
<td></td>
<td>The personal data has been collected when providing information society services (for example, e-commerce or e-government) to a child</td>
</tr>
</tbody>
</table>

Unlike LLPPD, the Regulation sets an additional requirement for the controller who first made the personal data being processed public. If the request to erase data is justified, the obligation to erase it extends beyond the controller’s own media – the controller must also inform other controllers of the fact that said person desires to have their data erased. The form and method of notification should be selected by taking account of the available technologies, the cost of implementation and what is reasonable.82

Here’s an example of exercising the right to erasure: someone wrote about their noisy neighbours on their blog, providing their name, occupation, age and address. They did not have the neighbour’s consent to publish such data.83 The blog post was shared on a social network and later published on news sites. The neighbours may request that the blogger not only remove the entry, but also ask the other entities, namely, the social network and the news sites, to erase the data.
However, this is not an absolute right. The controller may refuse to satisfy a request if it is necessary for exercising the right of freedom of expression and information, if specific personal data is being processed to comply with a legal obligation, to perform a task carried out in the exercise of official authority vested in the controller or for reasons of public interest in the area of public health, as well as for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for defending a legal claim.84

When it comes to right to be forgotten, bloggers have their tongues firmly planted in cheek – after all, “1984, the famous novel by English writer George Orwell, was meant to serve as a warning, not an instruction manual.” This right became the centre of discussion in 2014, when the Court of Justice of the European Union delivered its ruling in Google v Spain.85 The Court held that persons can ask Google and other search engines remove links to published information concerning them if this information is “inadequate, irrelevant or no longer relevant, or excessive”. Search engines are under an obligation to remove such links, although the information is still available on the actual websites (news sites, blogs et al.). This is not an absolute right, as search engine may refuse to delete a link if it is necessary for exercising the right of freedom of expression.86

84 Art. 17(3) of the Regulation


Right to restriction of processing

Just like the LLPPD, the Regulation provides for the person’s right to temporarily suspend the processing of their data. The Regulation features an expanded list of circumstances in which a person may request for this to be done:

<table>
<thead>
<tr>
<th>Law on Legal Protection of Personal Data</th>
<th>General Data Protection Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The data is incorrect, incomplete or inaccurate</td>
<td>The data is incorrect, incomplete or inaccurate during the period it is being checked</td>
</tr>
<tr>
<td>Data is being processed unlawfully, unfairly</td>
<td>The processing is unlawful but the data subject opposes the erasure</td>
</tr>
<tr>
<td></td>
<td>The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims</td>
</tr>
<tr>
<td></td>
<td>The data subject has objected to processing – pending the verification of his claim</td>
</tr>
</tbody>
</table>

The Regulation does not establish a minimum or maximum period for the suspension of processing, since that depends on the situation. During this period, companies may not process personal data (with the exception of storage), unless the situation falls under one of the exceptions.89

Right to data portability

The right to data portability did not previously exist under the LLPPD and was introduced by the Regulation.80 It aims to ensure that individuals can freely transmit their data between different service providers, for example, between different social networks or email providers. In essence, this right is similar to phone number portability, which is available in Lithuania: consumers are able to switch their landline or mobile service provider and keep their existing phone numbers. Consumers ask the new provider to transfer their old phone number, with the new provider being required to do so for free.81

The right to data portability may be exercised when the data provided by subjects is automatically processed with their consent or in pursuance of a contract (see section titled “The current regulatory regime governing the protection of personal data in Lithuania”). This right is unavailable if data is being processed on other grounds. It may be exercised in one of two ways:

- the person asks a company to provide him or her with the data in a structured, commonly used and machine-readable format (for example, a CSV file)82 and then forwards it to another company him- or herself
- the person asks a company to transmit his or her data to another company (if technically feasible)

Since it is not entirely clear how the right to data portability should be implemented, the Article 29 Data Protection Working Party is planning to release guidelines on its implementation in the near future.83

80 Art. 20 of the Regulation
81 The conditions and procedure for ensuring the right of subscribers to retain their contract phone number when switching to another public phone network, changing the location for or the method of the provision of services, have been approved by Order No. 1V-460 of the Director of the Communications Regulatory Authority, dated 29 April 2011, https://www.e-tar.lt/portal/lt/legalAct/TAR.75728E995F8A/TAIS_470604
Right to object to the processing of data

The Regulation also provides for yet another LLPPD right, namely, the right to object, on grounds relating to that person’s particular situation, to the processing of personal data.94 As before, it is available in three situations:

- when data is being processed in the exercise of official authority
- when data is being processed for the purposes of a legitimate interests pursued by the controller or by a third party
- when data is being processed for direct marketing purposes (e-mail adverts, phone calls offering goods or services)

In the first two cases the person’s request should be granted, that is, the company should stop processing unless it falls under an exception, which must be demonstrated by the company.95 If persons no longer want to have their data processed for direct marketing purposes (for example, they no longer want to receive newsletters), their wishes must be observed without exception.

While the controller is deciding on how to give effect to the right, the person may request to have processing suspended for that period (see the section titled “Right to restriction of processing”).

Profiling

Although the LLPPD provides for an automated decision-making, for the first time ever, the Regulation provides a definition for profiling. Profiling means any form of automated processing (whether by computer or an analogous system) of personal data consisting of the use of personal data to evaluate and/or predict a person’s behaviour, performance at work, economic situation, health, interests and so on.96 Most companies promoting products or services on Facebook rely on profiling, targeting persons of a particular gender and age that have specific interests. For example, a company selling tracksuits for men in advertising that reaches out exclusively to men interested in sports.

In certain cases, decisions based on profiling may have legal repercussions or otherwise affect a person. For example, suppose a person applies for a loan on a website. The site’s algorithm automatically assesses their personal data, including the information available on their social networks, and immediately rejects the application.

Such decisions may only be taken in three cases:

<table>
<thead>
<tr>
<th>Law on Legal Protection of Personal Data97</th>
<th>General Data Protection Regulation98</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is authorized by law which also lays down suitable measures to safeguard the data subject’s legitimate interests</td>
<td>It is authorized by law which also lays down suitable measures to safeguard the data subject’s legitimate interests</td>
</tr>
<tr>
<td>If the decision is taken when entering into or performing a contract, in response to the data subject’s request to enter into or perform a contract</td>
<td>It is necessary for entering into, or performance of, a contract between the data subject and a data controller</td>
</tr>
<tr>
<td>If the decision is taken when entering into or performing a contract, if safeguards are put into place to protect the data subject’s legitimate interests</td>
<td>It is based on the data subject’s explicit consent</td>
</tr>
</tbody>
</table>

94 Art. 21 of the Regulation, Art. 27 of the LLPPD
95 “The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims” Art. 21(1) of the Regulation.
96 Art. 4(4) of the Regulation
97 Art. 28 of LLPPD
98 Art. 22 of the Regulation
The Regulation provides that if the decision was taken in pursuit of a contract or based on the data subject's consent, the subject has the following rights:

- to demand human intervention on the part of the controller adopting the decision
- to express his or her point of view regarding the decision
- to contest the decision

Continuing the above example, the person may contest the automated decision with the site's management and provide additional information. A member of staff, after assessing the information provided, may then alter the automated decision.

**Remedies**

Just like before, if a person believes that his or her rights have been violated (for example, they received no reply from the controller regarding a request to access data), he or she is able to complain to a data protection supervisory authority. In Lithuania, that's the State Data Protection Inspectorate. Upon finding a breach, the authority may order companies to carry out certain actions (for example, to provide the person with data) or issue a fine.

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. 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.

---

99 Art. 22(3) of the Regulation

100 Depending on the facts, an employee may leave the automated decision unaltered. As an example, see analogy with Information Commissioner’s Office, “Automated decision making”, ico.org, (date unspecified), https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/automated-decision-taking/

101 Under Art. 12(3) of the Regulation, the controller must provide this information within one month of receipt of the request (under the LLPPD, it's within 30 days of the request); that period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The same timeframe applies when responding to other requests from data subjects.

102 Art. 58 of the Regulation


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.105 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”).106 The Regulation does not set a minimum fine, leaving that to the Member States.

If the person is unsatisfied with the data protection authority's response, if the institution does not handle the complaint or does not inform the person of the progress or outcome of the complaint within three months of the complaint, the Regulation provides for the right to an effective judicial remedy against the authority's decision or actions.107 Judicial proceedings are also necessary if a person seeks to obtain pecuniary or non-pecuniary relief for the violation of his or her rights. In that case, the defendant is the company responsible for the breach.108

It has been found that persons without legal qualifications who are unable to obtain legal aid are reluctant to seek redress for data security breaches.109 To this end, the Regulation, unlike the LLPPD, provides that individuals in personal data supervisory authority or court hearings may be represented by NGOs or associations active in the field of data protection.110

105 Art. 83(5) of the Regulation
106 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/4ebe66c0262311e5bf926a3f6a2e8b1ujpyH/Vrijb
107 Art. 78 of the Regulation
108 Art. 79 of the Regulation
110 This right will be granted to organizations in all cases. If the Member State chooses to, organizations may be further allowed to represent persons in judicial proceedings for compensation and to submit complaints regarding security breaches with or without the data subject's request. (Art. 80 of the Regulation).
The study revealed the existence of the so-called “privacy paradox”: while three-quarters of Lithuanian residents claim that they find the right to data protection to be just as important as the freedom of expression, only a few show firm resolve to take action, such as paying a fee to ensure that their data is better protected.

Awareness of the right to data protection

One possible explanation for this paradox may be the lack of knowledge of one’s own rights. The study found that the Lithuanian public’s awareness of the right to data protection not only failed to grow in recent years, it actually declined slightly. Only one in five residents is aware of the right of access and even fewer know about the right to erasure.

Only 5 percent of all Lithuanian residents claim to be aware of the EU Data Protection Reform and the regulations coming into force in May 2018, with barely 1 in 5 respondents expressing an interest in finding out more. Most would prefer obtaining more information from the media or the Internet.

These results are natural, since, with the exception of a few initiatives,111 there are no systemic or widespread campaigns in Lithuania to explain the complex processes involved in data processing and empower residents to take control of them. Examples of such initiatives can be found among “My Privacy Diary” (Hungary),112 the EduGiodo educational platform (Poland),113 “Your Data – Your Concern” (Poland),114 the “You Decide” toolkits (Norway),115 “Me and My Shadow” (international),116 “Security in a Box” (international)117 and “Disconnect” (USA).118

In other countries, these educational projects are usually initiated by data protection supervisory authorities or NGOs specializing in the right to privacy. There are almost no such organizations in Lithuania and the public sector is fairly passive in the field of communication and education, possibly due to lack manpower and funding.

The Regulation stipulates that data protection supervisory authorities, inter alia, “promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing.”119 To ensure that the State Data Protection Inspectorate is able to carry out its new function120 in cooperation with state and non-governmental partners, the state should provide it with adequate resources. Otherwise, the rights under this Regulation risk becoming mere “paper” rights, with very limited practical effect on everyday life.

111 For example, www.draugiskasinternetas.lt; www.vartotojai.lt/lt/tapatybe/apie; manoteises.lt/zyma/skaitmenines-teises/


115 http://www.dubestemmer.no/en/voksne/teachers-and-others

116 https://myshadow.org/

117 https://securityinabox.org/

118 https://disconnect.me/icons

119 Art. 57(1)(b) of the Regulation

120 This function was not present under Art. 40 of LLPPD.
Weight given to the right of data protection

The study revealed that a fair portion of the population is not yet firmly decided on what concrete steps should be taken to protect the right to data protection, but would be willing to take care of it. For example, 41% of residents said that they are likely to change their service provider if it was in breach of data protection rules and 28% would probably pay a fee to their e-mail provider for better data protection.

These results should be evaluated in the context of the 2014 analysis by the European Data Protection Supervisor (EDPS). The EDPS analysis claims that consumers pay more attention to the protection of their data when it comes to financial services, health care and other similarly “sensitive” markets. Business companies operating in these markets invest in additional data security measures, since security breaches may adversely affect the company’s reputation and lead to a loss of customers.

Meanwhile, when it comes to “free” services (such as social networks, e-mail and so on), businesses tend not to think of data protection as a competitive advantage, since it is believed that consumers don’t pay much attention to the protection of their data. However, studies in the economics of privacy (and, in this case, our representative survey) suggest that this aspect can affect consumer preference between service providers.

In fact, the right to data portability, a new right introduced by the Regulation, actually aims to allow consumers to switch to a new service provider without losing previously shared personal data. According to the EDPS, the implementation of this right could contribute to greater competitiveness in the “free” services market and the development of technologies for ensuring privacy. Whether these expectations bear fruit depends, in particular, on consumer awareness, since only consumers that know their rights are able to make use of them.

Defending the right to data protection

Seeing that public awareness of their right to data protection is low, it is not surprising that 81% of people did not take action to defend their right when it was violated. Such passiveness is chiefly the result of not knowing which institution to go to in the event of a breach and the belief that any such action would be meaningless.

The 2014 study of the FRA revealed that, when defending their rights, victims of data breaches have different aims: to rectify or remove their data, to have offending party punished, to protect other persons. They can also be motivated by the desire to prevent similar violations in the future or wish get official confirmation that there was in fact a breach.

The first obstacle to overcome when defending one’s right to data protection is the aforementioned asymmetry of information – it is not clear in all cases what personal data is held by companies and how exactly that information is processed (for example, whether the data is sent to a third party or shared with other companies, how long it is retained, which company employees have access to it). The second hurdle is classifying actions. Educational shortcomings mean that the public is not able to correctly identify whether an action is a data breach in all cases. Thirdly, it is more difficult to obtain remedies (whether through DPAs or the courts) without a professional to represent one’s interests.

To empower data subjects, the Regulation provides that NGOs or associations active in the field of data protection may appear before personal data supervisory authorities or the court on another’s behalf. Given how passive the Lithuanian public is when it comes to defending its right to data protection, it is imperative that, when implementing the Regulation, organizations are given the ability to effectively represent data subjects in the proceedings, whether it be contained in the Code of Civil Procedure, the Code of Administrative Violations of the Law and/or a separate piece of legislation setting out the procedure for defending the right to data protection.

122 Ibid.
123 Ibid.
124 Ibid., p. 36