



universität
wien

MASTER THESIS

Titel der Master Thesis / Title of the Master Thesis

“Comparative study on consent in the General Data Protection Regulation and the Federal Law on Personal Data of the Russian Federation”

verfasst von / submitted by
Mag. Margarita Sukach

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of
Master of Laws (LL.M.)

Wien, 23. Oktober 2020 / 13 October 2020

Studienkennzahl lt. Studienblatt /
Postgraduate programme code as it appears on
the student record sheet:

A 992 548

Universitätslehrgang lt. Studienblatt /
Postgraduate programme as it appears on
the student record sheet:

Europäisches und Internationales Wirtschaftsrecht /
European and International Business Law

Betreut von / Supervisor

Dr. Lukas Feiler

Table of contents

Table of contents	2
Acknowledgements.....	5
Table of cases.....	6
European Union	6
Greece.....	6
Russia	6
Spain.....	6
Sweden.....	6
Table of legislation.....	7
International treaties	7
European Union	7
Russian Federation.....	8
Other	9
1. Introduction	10
1.1 Relationship between the Russian Federation and the European Union.....	10
1.2 Importance of data privacy.....	11
1.3 Protection of personal data	11
1.4 Personal Aspect.....	13
2. Method	14
3. GDPR	17
3.1. General requirements for consent	17
3.1.1. Notion of consent	17
3.1.1.1. Freedom of consent	18
3.1.1.2. Specific	19
3.1.1.3. Informed	20
3.1.1.4. Unambiguous	21
3.1.1.5. Statement or clear affirmative action.....	21
3.1.1.6. Explicit consent	22
3.1.1.7. Obligation to demonstrate consent.....	22
3.1.2. Withdrawal of consent.....	23
3.2. Specific circumstances for consent.....	23
3.2.1. Consent provisions for children	23
3.2.2. Data processing in the workplace.....	25
3.2.2.1. Recruiting process.....	26
3.2.2.2. Background checks.....	26

3.2.2.3.	E-mails and device monitoring.....	26
3.2.2.4.	CCTV	27
3.2.1.	Publicly available data.....	27
3.2.2.	Automated decision making	28
4.	PERSONAL DATA LAW	30
4.1.	General requirements for consent	30
4.1.1.	Notion of consent	30
4.1.1.1.	Freedom of consent	31
4.1.1.2.	Specific	31
4.1.1.3.	Informed	32
4.1.1.4.	Conscious	33
4.1.1.5.	Act of consent	34
4.1.1.6.	Written consent	34
4.1.1.7.	Obligation to demonstrate consent.....	35
4.1.2.	Withdrawal of consent.....	35
4.1.3.	Time limit for consent	36
4.1.4.	Consent by representative.....	36
4.2.	Specific circumstances for consent.....	37
4.2.1.	Consent provisions for children	37
4.2.2.	Data processing in the workplace	38
4.2.2.1.	Recruiting process.....	40
4.2.2.2.	Background Checks	40
4.2.2.3.	E-mails and device monitoring.....	41
4.2.2.4.	CCTV	41
4.2.3.	Publicly available data.....	42
4.2.4.	Automated decision making	43
5.	COMPARISON.....	44
5.1.	General requirements for consent	44
5.1.1.	Notion of consent	44
5.1.1.1.	Freedom of consent	45
5.1.1.2.	Specific	48
5.1.1.3.	Informed	49
5.1.1.4.	Unambiguous	50
5.1.1.5.	Conscious	51
5.1.1.6.	Act of consent	51

5.1.1.7.	Reinforced consent	52
5.1.1.8.	Duty to demonstrate consent	53
5.1.2.	Withdrawal of consent.....	54
5.1.3.	Time limitation	56
5.1.4.	Consent by representative	57
5.2.	Specific circumstances for consent.....	58
5.2.1.	Consent provisions for children	58
5.2.2.	Imbalance of Power	58
5.2.3.	Data processing in a workplace	59
5.2.3.1.	Recruiting process.....	61
5.2.3.2.	Background checks.....	62
5.2.3.3.	E-mails and device monitoring.....	62
5.2.3.4.	CCTV	63
5.2.4.	Publicly accessible data.....	63
5.2.5.	Automated decision making	64
5.2.6.	Can consent be harmful?	65
6.	CONCLUSION.....	67
7.	Bibliography	70
8.	Articles	70
9.	Annex 1: Abstract (English)	71
10.	Annex 2: Zusammenfassung (German summary).....	72

Acknowledgements

I would like to thank my family for supporting me throughout my studies. Special thanks to my partner Stewart for words of encouragement and proofreading and to our daughter Ellie for giving me the motivation to finish this thesis.

Table of cases

European Union

European Court of Human Rights

Bărbulescu v Romania [2017] 61496/08	27
--	----

ECJ

Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH [2019]	52
--	----

Greece

Hellenic Data Protection Authority (HDPА) v PriceWaterhouseCoopers [2019] 26/2019	15, 61, 65
---	------------

Russia

Определение Арбитражного суда Поволжского округа от 4 сентября 2017 г. N Ф06-25228/17 по делу N А65-4208/2017	32, 48
Определение Верховного Суда РФ от 29.01.2018 N 305-КГ17-21291 по делу N А40-5250/2017	43
Определение Московского городского суда от 10.11.2016 по делу N 33-38783/2016 (LinkedIn Russia Case)	15
Постановление Арбитражного суда Северо-Западного округа от 18 июля 2016 г. N Ф07-5537/2016 по делу N А44-9647/2015	33
Постановление Одиннадцатого арбитражного апелляционного суда от 17.07.2017 N 11АП-8208/2017 по делу N А65-4208/2017	32-33, 46, 49
Постановление Одиннадцатого арбитражного апелляционного суда от 15.01.2018 N 11АП-17453/2017 по делу N А65-25979/2017	45
Постановление Одиннадцатого арбитражного апелляционного суда от 16 января 2017 г. N 11АП-17453/16	52-52
Решение Арбитражного суда города Москвы от 5 мая 2017 года по делу № А40-5250/17-144-51	43
Решение Арбитражного суда Республики Бурятия от 09.07.2012 по делу N А10-125/2012	56
Решение Псковского городского суда Псковской области от 30 октября 2014 г. по делу № 2-3512/2014	47, 66

Spain

Lopez Ribalda and others v Spain Applications 1874/13 and 8567/13	27
---	----

Sweden

Swedish Data Protection Authority v Google [2020] DI-2018-9274	15
--	----

Table of legislation

International treaties

Convention on the Rights of the Child	2423
Partnership and Cooperation Agreement between the European Communities and their Member States the Russian Federation.....	10

European Union

GDPR.....	1.311
------------------	--------------

Rec 11	21	Art 6 (1) lit b.....	62
Rec 32	18, 21	Art 6 (1) lit f.....	26, 62
Rec 38	23-25	Art 7 (1).....	22, 53
Rec 39	19	Art 7 (2).....	1920-21, 24, 49-50
Rec 40	17	Art 7 (3).....	19, 23, 54
Rec 42	18, 20, 22, 655	Art 8 (1).....	234, 588
Rec 43	18, 48	Art 9 (2).....	22, 26
Rec 47	27	Art 12 (1).....	24
Rec 58	234	Art 17 (1) lit b.....	545
Rec 65	23	Art 17 (2) lit d.....	56
Rec 155	25, 61	Art 17 (3).....	23
Art 4 (7).....	44	Art 22.....	28
Art 4 (11).....	17, 21	Art 22 (2).....	29
Art 5 (4).....	62	Art 22 (2) lit c.....	22, 29
Art 6.....	6054	Art 22 (3).....	29, 65
Art 6 (1).....	17, 44-45	Art 49 (1) a.....	22, 49

Consolidated version of the Treaty on the Functioning of the European Union	
Art 26 para 6	10

Charter of Fundamental Rights of the European Union	
Art 8	11

Data Protection Directive	25
---------------------------------	----

Opinions

Opinion on the Definition of Consent.....	12, 17-20, 25, 44, 47-48, 522, 61
Opinion on some key issues of the Law Enforcement Directive (EU 2016/680).....	28-29, 59
Opinion on Data Processing at Work	25

Guidelines

Guidelines on Automated individual decision-making and Profiling	22, 25, 28-29, 64
Guidelines on Consent.....	18-23, 27, 46, 49, 54, 56-58, 65
Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data	18, 58
Guidelines on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.....	65

Other

Working Document on the processing of personal data relating to health in electronic health records	18
Information Commissioner's Office, 'Consultation: GDPR consent guidance' [2017].....	53, 57, 68

Russian Federation

О персональных данных: федер. закон Рос. Федерации (Personal Data Law)..... 124

Art 1 (2) 2.....	56	Art 9 (3).....	35, 42, 53
Art 3 (1).....	30	Art 9 (4).....	33-34, 36, 50, 53
Art 3 (2).....	30, 44	Art 9 (6).....	37
Art 3 (3).....	30, 33	Art 10.....	37
Art 5 (7).....	36	Art 10 (1) 3.....	65
Art 6 (1).....	30, 44	Art 10 (2) 1.....	35
Art 6 (2).....	30, 44	Art 10 (2) 2.....	43
Art 6 (10).....	412	Art 11 (2).....	42
Art 8.....	42	Art 12 (4) 1.....	34
Art 8 (1).....	35, 43, 63	Art 16 (1).....	43
Art 9.....	41, 48	Art 16 (2).....	35, 43
Art 9 (1).....	31-32, 34-36, 45, 50, 53-54	Art 16 (3).....	43, 64
Art 9 (2).....	345, 48, 55	Art 21 (5).....	35

О внесении изменений в отдельные законодательные акты Российской Федерации в части проведения государственной дактилоскопической регистрации в Российской Федерации: федер. закон Рос. Федерации от 31.12.2017 N 498-ФЗ..... 12

О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях: федер. закон Рос. Федерации от 21.07.2014 г. № 242-ФЗ.. 12

О внесении изменений в Федеральный закон "О персональных данных", законопроект № 305068-7..... 37

Гражданский кодекс Российской Федерации (Civil Code)

Art 21 (1).....	37	Art 27 (1).....	37
Art 26 (1).....	37	Art 185-186.....	36

Гражданский процессуальный кодекс Российской Федерации 35

О государственной гражданской службе Российской Федерации: федер. закон Рос. Федерации

Глава 7.....	39
--------------	----

Об электронной подписи: федер. закон Рос. Федерации 34

Конституция Российской Федерации (Constitution of the Russian Federation)

Статья 24 (Article 24).....	11, 30, 33
-----------------------------	------------

Трудовой кодекс Российской Федерации (Labour Code)

Art 22.....	38	Art 86 (6).....	40
Art 61 (1).....	40	Art 88.....	39, 59-61
Art 74.....	41	Art 372.....	38
Art 86 (1).....	38, 60	Section 14.....	39
Art 86 (3).....	59		

Government decrees

Постановление Правительства РФ от 21.03.2012 N 211 (ред. от 06.09.2014).....	34, 54
Постановление Правительства РФ от 15.09.2008 N 687	32, 34

Documents issued by Roskomnadzor

Разъяснения „Вопросы, Касающиеся Обработки Персональных Данных Работников, Соискателей На Замещение Вакантных Должностей, А Также Лиц, Находящихся В Кадровом Резерве“.....	38, 40, 56, 59, 61-62
Разъяснения „О Вопросах Отнесения Фото- И Видео- Изображения, Дактилоскопических Данных И Иной Информации К Биометрическим Персональным Данным И Особенности Их Обработки	42

Other

Austria

Bundesgesetz vom 14. Dezember 1973 betreffend die Arbeitsverfassung	27
---	----

Germany

Deutsches Bundesdatenschutzgesetz.....	25, 53
--	--------

Hungary

Hungarian Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.....	24
--	----

Netherlands

Dutch Data Protection Law, Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens);.....	24
---	----

Spain

Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.....	24
---	----

1. Introduction

1.1 Relationship between the Russian Federation and the European Union

At the time of writing, the European Union is a political and economic union that consists of 27 member states with a total population of 446 million inhabitants¹. The EU has established an internal single market that comprises of an area without internal frontiers in which the free movement of goods, persons, services, and capital is ensured.²

Russia is the world's largest country, spreading over 17.08 million km². It has a population of 146.8 million people³ and a gross domestic product of RUB 109,361.5 billion⁴. The EU and Russia have traditionally been important trading partners, especially in the energy sector. According to the European Commission, the trade in goods between Russia and the EU is estimated to be EUR 253 billion in 2019.⁵

In 1994, the Russian Federation and the European Communities signed a Partnership and Cooperation Agreement⁶ that is fundamental to the bilateral relationship between the two parties. Apart from its symbolic importance, the Partnership and Cooperation Agreement has been aiming to establish a strategic partnership, facilitate trade, support the economic relations, and encourage investment.

Even though the relationship between the EU and the Russian Federation has changed over the years, Russia is and remains a strong economical player. It remains an important market for companies based in the EU.

¹ Anon 'EU in figures' (10 February 2020) <https://europa.eu/european-union/about-eu/figures/living_en> accessed 28 March 2020

² Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/59 (TFEU) art 26 para 2

³ Росстат, 'Оценка численности постоянного населения РФ (на 01.01.2020)' [2020] <<https://showdata.gks.ru/report/278928/>> accessed 28 March 2020

⁴ Росстат, 'Объем ВВП в текущих ценах за 2019г. (первая оценка)' [2020] <<https://showdata.gks.ru/report/280029/>> accessed 28 March 2020

⁵ European Commission on Russia on 13 Nov 2019 <<https://ec.europa.eu/trade/policy/countries-and-regions/countries/russia/>> accessed 28 March 2020

⁶ Council and Commission Decision of 30 October 1997 on the conclusion of the Partnership and Cooperation Agreement between the European Communities and their Member States, of the one part, and the Russian Federation, of the other part, 97/800/ECSC, EC, Euratom [1997] OJ L 327/1

After the fall of communism in 1991, Russia fully reformed its legal doctrine. When creating the new paradigmatic framework, Russia once again took its influences from the West.⁷ Despite the inspirations drawn from continental Europe, there are some crucial differences between the Western and Russian legal systems, especially when legal practice is concerned.

1.2 Importance of data privacy

In the last few decades, the protection of personal data has gained significant importance. The internet and other technological developments have enabled a seamless cross-border flow of information, the ability to connect online and unstoppable globalization. The media has dubbed this the digital or information age.⁸

Despite all the positive aspects of an ever-increasing interconnect world, there are downsides. Information, specifically personal data, has become a trade good, individuals are losing control over their personal data and privacy is disappearing. Many countries globally have now recognized the importance and need for the protection of an individual's right to data privacy.

It is not surprising that the Russian Federation has named privacy a constitutional right,⁹ while the European Union included privacy into the list of human rights.¹⁰

1.3 Protection of personal data

On 27 April 2016, the General Data Protection Regulation¹¹ was passed into regulation by the European Parliament and is now directly applicable across the EU since 25 May 2018. In

⁷ Mark Van Hoecke, 'Methodology of Comparative Legal Research' [2015] Law and Method, December 2015, DOI: 10.5553/REM/.000010, page 25

<<https://www.bjutijdschriften.nl/tijdschrift/lawandmethod/2015/12/RENM-D-14-00001>> accessed 25 March 2020

⁸ Cambridge University Press, 'digital age, n', *Cambridge Business English Dictionary* <<https://dictionary.cambridge.org/de/worterbuch/englisch/digital-age>> accessed 28 March 2020

⁹ Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 года. : (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ 30 декабря 2008 № 6-ФКЗ и № 8 – ФКЗ) // Собр. законодательства РФ. - 2014. - № 31 - Ст. 4398 (**Constitution of the Russian Federation**) // Art 24

¹⁰ Charter of Fundamental Rights of the European Union [2012] OJ C 326/391, art 8

¹¹ Regulation 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 (General Data Protection Regulation) [2016] OJ L 119, p. 1-88 (**GDPR**)

particular, the GDPR aims to unify the protection of personal data in the EU and therefore facilitate the transfer of personal data within the Union.

The Law on Personal Data of the Russian Federation¹² was adopted by the State Duma on 26 July 2006 and has been amended several times since, with the latest amendment coming into force on 31 December 2017.¹³ To date the most discussed amendment of the law was implemented with the Federal Law No. 242-FZ that came into force on 1 September 2015.¹⁴ Specifically, this amendment requires legal entities processing personal data to use databases that are physically located in the Russian Federation for the processing of personal data relating to Russian citizens.

It is safe to say that virtually any company processes personal data in one way or other. In addition, it is more likely than not that a company processing personal data needs to adhere to privacy laws of more than one jurisdiction. With an increasing amount of varying regulations across jurisdictions, it has become difficult for companies operating internationally to ensure full compliance.

Consent is probably the most important and most discussed topic when thinking of processing personal data in both jurisdictions.¹⁵ The notion of consent in data privacy and its applicability may differ dramatically from jurisdiction to jurisdiction. For the above reasons I decided to undertake this explanatory comparative research, which enabled me to contrast the concept of consent regarding the privacy law of the Russian Federation on one side and on the level of the European Union on the other side.

¹² Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных": принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г.: редакция от 22.02.2017 // Собр. законодательства РФ. - 2017. - № 9 - Ст. 1276 Раздел I (**Russian Data Privacy Law**)

¹³ Федеральный закон от 31.12.2017 N 498-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части проведения государственной дактилоскопической регистрации в Российской Федерации": принят Гос. Думой Федер. Собр. Рос. Федерации 20 декабря 2017 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 26 декабря 2017 г. // Собр. законодательства РФ. – 2018. – № 1 (Часть I) – Ст. 82

¹⁴ Федеральный закон от 21.07.2014 г. № 242-ФЗ „О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях“: принят Гос. Думой Федер. Собр. Рос. Федерации 4 июля 2014 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 9 июля 2014 г. // Собр. законодательства РФ. - 2014. - № 30 - Ст. 4243 Раздел I

¹⁵ Article 29 Working Party, Opinion 15/2011 on the definition of consent [2011] WP187 (**Opinion on the Definition of Consent**)

1.4 Personal Aspect

I wanted to write this master thesis due to my personal connection to the topic. I work as a Legal Counsel in an international IT company. My focus lies with the legal support of Austria, Eastern Europe and Russia. I speak Russian, English and German fluently. I am specifically interested in Data Protection and following a review of legal materials from different countries, I became interested in the similarities and differences in the approach to data protection. I wondered if it was possible for a company to create one policy on consent for processing of personal data that could be applicable across several jurisdictions and whether such a decision would be desirable in the context of business reality, as well as in the context of the privacy laws in question.

2. Method

In this master thesis, I undertook a comparative study on the instrument of consent in the General Data Protection Regulation and the Federal Personal Data Law of the Russian Federation. In order to make this comparison, I was using the elements of the functional method and the law-in-context method of comparative law.

To create a micro level comparison of the concept of consent, I addressed each characteristic of the instrument separately. In this way, I separately compared the notion of consent and each of its elements as well as consent in specific circumstances. The latter includes consent provisions for children, data processing in the workplace, publicly available data and automated decision making.

To undertake an effective academic legal comparison, I had to find a neutral point of reference to which I could compare the relevant provisions of both jurisdictions. I have defined a “universal problem”¹⁶ and compared how the laws of the jurisdictions under comparison behave in the light of this *tertium comparationis*.¹⁷

For the purposes of this master thesis, I had to assume that a functional relationship between law and surrounding society exists and therefore the societal problem examined in this thesis does in fact trigger an adequate legal response.¹⁸ Furthermore, I had to assume that the problem I have chosen as my *tertium comparationis* is in fact consistent in both the European Union and the Russian Federation.

Even though the concept of privacy is not new, there have been radical developments in this area, especially as a reaction to societal (increasing importance of social media) and scientific developments (new technologies enabling a mass processing of data). Online society and international enterprises make privacy a global concern.

¹⁶ Julie De Coninck, ‘The Functional Method of Comparative Law: *Quo Vadis?*’ [2010] The Rabel Journal of Comparative and International Private Law Bd. 74, H. 2 (April 2010) 318 <<https://www.jstor.org/stable/27878873?seq=1>> accessed 29 March 2020, page 329

¹⁷ *ibid* 323

¹⁸ *ibid* 333

One of the central considerations regarding the topic of privacy is the individual's ability to have control over their personal data. The instrument of consent provides the means for the data subject to exercise such control.

Given the above, I believe that the problem defined above may be presumed similar and therefore render the provisions regarding consent in the GDPR and in the Personal Data Law comparable.

I have chosen to investigate how a legal entity processing data in the EU, and in Russia, can comply with the requirements of consent in each jurisdiction simultaneously. One of the questions I will be answering is whether a legal entity, being subject to both of the compared laws, can introduce one consent policy that can comply with the provisions of both laws at the same time. If one consent policy is not possible due to different or contradicting requirements set out by Personal Data Law and the GDPR, I will investigate the main aspects of each law that the entity processing personal data needs to adhere to.

This study is undertaken to research the application of the GDPR and the Personal Data Law in the practical environment and the impact these laws have on entities processing personal data. Given that non-compliance with personal data laws can have dire consequences for the business of a company,¹⁹ it is in the interest of a company processing personal data to ensure conformity with the laws in this regard.

During my comparison, I will be describing the similarities of the concept of consent and pay special attention to the differences between mechanisms. In addition to the comparison of wording in the laws, I made use of case law as well as legal doctrine. I have also considered the application of the provisions in its "paradigmatical framework".²⁰

The thesis consists of three main sections. In the first section, I will break down the provisions of GDPR that relate to the concept of consent into its elements and discuss these elements separately. In the second section, I will undertake the same analysis with the relevant provisions of the Personal Data Law. The third and main section of the thesis will compare and analyze

¹⁹ Определение Московского городского суда от 10.11.2016 по делу N 33-38783/2016 (**LinkedIn Russia Case**); Hellenic Data Protection Authority v PriceWaterhouseCoopers [2019] 26/2019; Swedish Data Protection Authority v Google [2020] DI-2018-9274

²⁰ Mark Van Hoecke, 'Methodology of Comparative Legal Research' [2015] Law and Method, December 2015, DOI: 10.5553/REM/.000010, page 25
<<https://www.bjutijdschriften.nl/tijdschrift/lawandmethod/2015/12/RENM-D-14-00001>> accessed 25 March 2020

the preceding two. In the latter comparison section, I intend to investigate similarities and differences, not just in the wording of the law, but also in its application, paying particular attention to business reality and practice.

3. GDPR

In this section, references to the law, unless otherwise indicated, shall mean the General Data Protection Regulation.

3.1. General requirements for consent

3.1.1. Notion of consent

Consent is one of six general legal grounds for the processing of personal data in accordance with the GDPR.²¹ Consent is also used as a specific processing ground for contexts explicitly provided for in the GDPR or national laws, e.g. as it is described in Articles 8 (2) lit a and 26 (1) GDPR.

Consent is the weakest processing ground and shall only be used if no other processing ground is applicable.²²

The purpose of consent is to give the “data subject control over the processing of his data”.²³ As stated in the Opinion 15/2011 of the Article 29 Working Party “an individual’s decision to accept a data processing operation should be subject to rigorous requirements, particularly taking into account that in doing so, an individual may be waiving a fundamental right”.²⁴ Obtaining a data subject’s consent does not free the data controller from other obligations under the law.²⁵

The definition of consent names several elements that must be fulfilled to render consent valid.²⁶ Although the elements are closely interlinked, it is vital to look into each of the elements separately as by not fulfilling one of them the consent may be invalid.

In the following section, each of the elements will be examined separately.

²¹ Art 6 (1) GDPR

²² Opinion on the Definition of Consent 10

²³ *ibid* 2

²⁴ *ibid* 3

²⁵ Rec 40 GDPR

²⁶ Art 4 (11) GDPR

3.1.1.1. Freedom of consent

As mentioned above, the main objective of consent is giving the data subject control over their data. According to the Council of Europe, “[c]ontrol requires awareness of the use of personal data and real freedom of choice.”²⁷

Giving the data subject a genuine choice about the processing of their data, means that the consent shall not be a precondition of a service unless it is necessary for such service (the same applies for treatment, employment, etc.).²⁸ Consent is only free if it is possible for the individual to make a decision without any negative consequences.²⁹ Any “element of inappropriate pressure or influence”³⁰ make it impossible for the consent to be free.

However, this does not exclude the possibility of the controller to provide an incentive for the data subject to provide consent.³¹ Such incentives should only be valid if the controller can prove that the consent was still given freely in all circumstances.³²

The instrument of consent should only be used where it is possible for the data subject to make a “voluntary decision by an individual in possession of all of his faculties”³³. Otherwise, the request to provide consent can be “misleading or inherently unfair”.³⁴

The individual should be able to consent to various kinds of processing separately.³⁵ Feiler and Fórgo refer to this requirement as the “Prinzip der gesonderten Einwilligung” (translated: principle of separate consent).³⁶

²⁷ Council of Europe, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data [2017] T-PD 1

²⁸ Rec 43 GDPR

²⁹ Rec 42 GDPR

³⁰ Article 29 Working Party, Guidelines on consent under Regulation 2016/679 [2017] revised in 2018 (**Guidelines on Consent**) 6

³¹ See “moderate financial incentive” in Opinion on the Definition of Consent 15

³² Guidelines on Consent 11

³³ Article 29 Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR) [2011] WP131 8

³⁴ Opinion on the Definition of Consent 13

³⁵ Rec 32 and 43 GDPR

³⁶ Lukas Feiler and Nikolaus Forgó ‘EU-DSGVO: EU-Datenschutz-Grundverordnung: Kurzkomentar’ [2017] Verlag Österreich 12

Freedom of consent includes the right to withdraw the consent at any time.³⁷ Such withdrawal does not have a retroactive effect on processing that has already taken place. However, presuming there are no other legal grounds for processing, the controller may have to delete or destroy any data gathered from the individual after the consent has been revoked. This is discussed in more detail during Chapter 3.1.2 Withdrawal of consent.

Guidelines on Consent mention several of Article 29 Working Party's opinions in which the limits of free consent have been explored.³⁸ Specifically this happened in Opinion 15/2011 on the definition of consent (WP 187) and Opinion 8/2001 on the processing of personal data in the employment context (WP48) to name a few.

3.1.1.2. Specific

Specific consent means the permission of the data subject to process their data in a particular way for an identified legitimate purpose. According to Article 29 Working Party's Guidelines on consent, the criterion of specific consent includes "(i) [p]urpose specification as a safeguard against function creep, (ii) [g]ranularity in consent requests, and (iii) [c]lear separation of information related to obtaining consent for data processing activities from information about other matters."³⁹

The data controller has the obligation to identify a "specific, explicit and legitimate purpose for the intended processing activity".⁴⁰ Naturally, the data subject needs to be provided with information regarding the purpose of processing and its consequences. As a result, it is safe to say that only an informed decision can be specific.

According to Rec 39 GDPR, "[p]ersonal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means". Article 29 Working Party states that processing must be "reasonable and necessary in relation to the purpose".⁴¹

As mentioned in section 3.1.1.1 above, a separate consent must be obtained for each processing activity. This criterion is often referred to as the requirement of granularity. Article 29 Working

³⁷ Art 7 (3) GDPR

³⁸ Guidelines on Consent, page 5

³⁹ Guidelines on Consent 11

⁴⁰ Guidelines on Consent 12

⁴¹ Opinion on the Definition of Consent 17

Party defines granularity as “separation of [...] purposes and obtaining consent for each purpose”.⁴²

If request for consent is presented as a part of a document concerning other issues (e.g. general terms and conditions), “the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language” (Art 7 (2) GDPR).

3.1.1.3. Informed

Article 29 Working Party states in its Opinion 15/2011 that „[t]ransparency is a condition [...] for rendering consent valid.”⁴³ According to Art 7 (2) GDPR the “request for consent shall be presented [...] in an intelligible and easily accessible form, using clear and plain language”.⁴⁴

Before giving their consent, the individual has to obtain a minimum set of information. Article 29 Working Party summarized the information which has to be provided to the data subject for obtaining a valid consent as follows:

- “(i) the controller’s identity,
- (ii) the purpose of each of the processing operations for which consent is sought,
- (iii) what (type of) data will be collected and used,
- (iv) the existence of the right to withdraw consent,
- (v) information about the use of the data for automated decision-making in accordance with Article 22 (2) lit c where relevant, and
- (vi) on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46”.⁴⁵

The requirement of an informed consent is closely linked to the information notice obligations described in Art 12-14 GDPR. However, the provision of information notices is not a necessary requirement for a valid consent.⁴⁶

⁴² Guidelines on Consent 10; see also “Prinzip der gesonderten Einwilligung” in Lukas Feiler and Nikolaus Forgó ‘EU-DSGVO: EU-Datenschutz-Grundverordnung: Kurzkomentar’ [2017] Verlag Österreich 12

⁴³ Opinion on the Definition of Consent 9

⁴⁴ Rec 42 GDPR

⁴⁵ Guidelines on Consent 13

⁴⁶ Lukas Feiler and Nikolaus Forgó ‘EU-DSGVO: EU-Datenschutz-Grundverordnung: Kurzkomentar’ [2017] Verlag Österreich 13

3.1.1.4. Unambiguous

According to GDPR's definition of consent contained in Art 4 (11) GDPR, consent shall be an "unambiguous indication of the data subject's wishes". This means a clear action set by the data subject as a manifestation of their consent.

Data controller would also be well advised to take into consideration a potential "click fatigue"⁴⁷ on the side of the data subject. Overloading the data subject with too many questions in an online environment may be confusing or simply overwhelming for the data subject. This may lead the data subject to clicking "Agree" thoughtlessly.

The controller needs to be able to clearly demonstrate that the data subject has actively agreed to the data processing.

According to Art 7 (2) GDPR, should the data subject's consent be given in the context of a written declaration which also concerns other matters, the request for consent should be presented in a manner that is clearly distinguishable from the other matters.

3.1.1.5. Statement or clear affirmative action

The GDPR does not have a specific form requirement for consent. Such indication can be a "written statement, including by electronic means, or an oral statement".⁴⁸ Consent may be expressed by setting a clear affirmative action that indicates the data subject's desire to agree.⁴⁹

The controller has the obligation to demonstrate consent, which may prove difficult when relying on non-recorded oral consent or affirmative action.

Inaction cannot be considered unambiguous consent. Therefore, controllers should be advised not to use pre-ticked boxes or default privacy settings. In the same way, "merely proceeding with a service cannot be regarded as an active indication of choice".⁵⁰

⁴⁷ Guidelines on consent 17

⁴⁸ Rec 32 GDPR

⁴⁹ Rec 11, 32 GDPR

⁵⁰ Guidelines on consent 16

3.1.1.6. Explicit consent

GDPR requires explicit consent “in certain situations where serious data protection risk emerge, hence, where a high level of individual control over personal data is deemed appropriate”.⁵¹

This construct goes further than a “simple” requirement of unambiguous consent by a statement or clear affirmative action. Such consent should leave no room for misinterpretation. Such consent cannot be implied and the individual needs instead to make a statement of agreement. While such a statement can be either oral or written, the controller needs to keep in mind the ability to demonstrate that such consent was provided at a later date.

In its guidance on consent, the Article 29 Working Party also considers two-stage verification as a valid explicit consent. A mere simple affirmative action is not considered to fulfil the criteria of the explicit consent.⁵²

Explicit consent is *inter alia* required for processing of sensitive data (Art 9 (2) lit a), automated individual decision-making, including profiling (Art 22 (2) lit c) and for transfer of personal data to third countries or international organisations in absence of adequate safeguards as required by Art 45 and 46 GDPR (Art 49 (1) a).

It is to point out that the processing of sensitive data is only allowed if an explicit consent has been obtained, even if such processing is necessary for the performance of a contract.⁵³ However, automated decision making including processing is allowed if necessary for the entering or performance of a contract or expressly authorised by law.⁵⁴ Should such processing, however, be based on consent, such consent needs to be explicit.

3.1.1.7. Obligation to demonstrate consent

Art 7 (1) GDPR obliges the controller to prove that consent was given in case the data controller is relying on consent as processing ground. Such obligation to demonstrate consent is also described in Rec 42 GDPR.

⁵¹ Guidelines on Consent 18

⁵² Guidelines on Consent 18

⁵³ *ibid* 19

⁵⁴ Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 [2017] WP251 (**Guidelines on Automated Decision-Making and Profiling**) 20

3.1.2. Withdrawal of consent

Consent should be a reversible decision.⁵⁵ According to Art 7 (3) GDPR the data subject has the right to withdraw their consent at any time. Revoking one's consent should be as easy as providing it. However, this does not mean that providing and withdrawing consent should be done by performing the same action.⁵⁶

After an individual's withdrawal of consent (and providing there is no other lawfulness ground which can be used) the controller loses the legal basis for processing such data subject's information. Whereas the data processing before the withdrawal remains unaffected, the controller may have to delete the data subject's data from its databases (cf Rec 65 GDPR).

Art 17 (3) GDPR provides for cases when personal data can continue to be processed even though the initial consent has been withdrawn.

Withdrawal of consent should be differentiated from the objection to processing. Objection to processing is a right of the data subject to prevent the controller from processing data on the basis of legitimate interest. This could be the case in a direct marketing scenario. Objection to processing of personal data is out of scope of this master thesis.

3.2. Specific circumstances for consent

Some processing activities require special rules due to their unique circumstances. The following chapter will discuss these exceptions.

3.2.1. Consent provisions for children

According to Rec 38 GDPR, children's data requires special protection, "as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."⁵⁷

Even though the GDPR recognizes that children require increased protection, the term child was not defined in the Regulation or otherwise on the level of EU legislation. The UN Convention on the Rights of the Child defines child as a "human being below the age of eighteen

⁵⁵ Guidelines on Consent 5

⁵⁶ *ibid* 21

⁵⁷ Rec 38 GDPR

years unless under the law applicable to the child, majority is attained earlier”.⁵⁸ This means that depending on the national laws the GDPR safeguards concerning children may be applicable to different age groups.

When relying on consent provided by a child, the controller needs to examine if such consent can be validly provided. Art 12 (1) as well as Rec 58 GDPR require notices to be understandable and clear for children, when they are directed to such. This provision is important to consider when identifying whether a consent given by a child is informed in line with Art 7 (2) GDPR. If this is not the case, such consent needs to be provided by the legal representative.

Since no clear guidance on the age of consent is provided by the GDPR, many EU countries decided to put provisions in place on national level. In Spain an individual may provide consent for processing of their data from the age of 14, unless a law specifically requires parents’ or legal guardian’s consent.⁵⁹ Netherlands⁶⁰ and Hungary⁶¹ require parental consent for minors under the age of 16. Other member states use the provisions of civil law by analogy, while the rest is encouraging the controllers to subjectively review each case to determine whether the minor had the mental capacity to validly provide consent for the particular processing operation at the time of the decision.

GDPR sees a need for special protection of children in an online environment. It therefore imposes an obligation to obtain parental consent for data processing in connection with information society services offered to individuals under 16 years of age.⁶² Member States may lower the age of consent down to the age of 13.⁶³ It is however to consider that “[t]he consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child”.⁶⁴

⁵⁸ United Nations, General Assembly Resolution 44/25, 20 November 1989 (**Convention on the Rights of the Child**)

⁵⁹ Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

⁶⁰ Article 5 Dutch Data Protection Law, Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens)

⁶¹ Section 6 sub-section 3 Hungarian Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information

⁶² Art 8 (1) GDPR

⁶³ *ibid*

⁶⁴ Rec 38 GDPR

According to Rec 38, children's personal data may not be used for purposes of automated decision making, including profiling. Article 29 Working Party, however, does not recognize this provision as an absolute prohibition, but rather urges controllers not to generally rely on the exceptions in Article 22 (2) when children's data is concerned.⁶⁵

3.2.2. Data processing in the workplace

In their opinion on data processing at work, Article 29 Working Party stated that in the majority of cases "consent cannot and should not"⁶⁶ be the correct legal ground for data processing of employees, unless the data subject can "refuse without adverse consequence".⁶⁷ This can particularly be the case if the employee fears to be treated differently⁶⁸ which can often happen in an employer-employee relationship.

It is important to mention here that GDPR, like the Data Protection Directive⁶⁹ before, uses a wide interpretation of the notion of "employee". In particular, this includes contractors and freelancers.

Interestingly, according to Rec 155 GDPR, Member States have the right to set specific rules on when consent can be used as legal ground for processing of personal data in an employment context. The new German Bundesdatenschutzgesetz 2018 used this right to introduce testing criteria to determine when consent is deemed to be free in an employment relationship.⁷⁰ It assumes the consent to be free if the aim of the processing activity is to provide the employee with a legal or economic benefit or if the employer and the employee pursue similar interests.⁷¹ While consent under the GDPR generally does not have to be in written form, under the German Bundesdatenschutzgesetz, the consent of employees concerning employment-related data processing will generally require written form.⁷²

⁶⁵ Guidelines on Automated Decision-Making and Profiling 28

⁶⁶ Article 29 Working Party, Opinion 02/2017 on data processing at work [2017] WP 249 (**Opinion on Data Processing at Work**) 6

⁶⁷ *ibid* 3

⁶⁸ Opinion on the Definition of Consent 13

⁶⁹ 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 [1995] OJ L281 31-50 (**Data Protection Directive**)

⁷⁰ Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 § 26 (1)

⁷¹ *ibid*

⁷² *ibid* § 26 (2)

3.2.2.1. Recruiting process

For reasons given in section 3.2.2 above, consent is rarely used as a lawfulness ground in the workplace environment. This also applies to the recruiting process.

Publicly accessible information of candidates should only be processed by a potential employer or recruiting agency if such data has been made public by the data subject for the purposes of being contacted by such entities. For example, a publicly accessible profile on the professional networking website LinkedIn is considered to be lawful due to user's general expectation to make work contacts through this website. However, it would be much harder to prove legitimate interest in searching other social media profiles of the data subject.

Should a recruiting agency or the potential employer wish to process sensitive personal data of a candidate (data subject), this requires explicit consent.⁷³

3.2.2.2. Background checks

Background checks by a potential or current employer should only be permissible if so authorized by law or there are strong reasons for processing of such data on the basis of legitimate interest. This may be the case if the (future) employee will be working in a sensitive environment. Prior criminal convictions may be of interest if the candidate is applying to work with vulnerable adults or children for example.

In the majority of cases, background checks will require a prior consent by the data subject. Such consent, however, will rarely be considered free, due to previously mentioned imbalance of power between the (potential) employer and the employee or candidate.

3.2.2.3. E-mails and device monitoring

The possibility of an employer to monitor devices depends on whether the employer allows the private use of company devices. Generally, company issued mobile phones and computers are company property. Where the employer prohibits the personal use of the company devices and can prove a legitimate interest in accordance with Art 6 (1) lit f GDPR, such monitoring can be permitted. It is also important to note that the legitimate interests of the employer cannot

⁷³ Art 9 (2) GDPR

outweigh the interests or the fundamental rights and freedoms of the data subject.⁷⁴ This was seen in the recent case *Bărbulescu v Romania*.⁷⁵

Where private use of company devices is permitted, the company would require explicit consent from the employees to monitor such devices.⁷⁶ Of course, the validity of such consent will depend on the ability of the employees to refuse the consent without any adverse consequence. In some countries like Austria and Germany, such monitoring would require an agreement with the works council.⁷⁷

3.2.2.4. CCTV

The most common processing ground for using CCTV by employers is legitimate interest. The processing ground of consent cannot be used in this circumstance due to imbalance of power between the employee and the employer and therefore the lack of freedom of consent. Article 29 Working Party was of the opinion that “[i]t is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera observation in a workplace”.⁷⁸

Even when the employer can prove a legitimate interest, the use of CCTV has to be limited to the utmost possible extent. This was shown in the case *Lopez Ribalda and others v Spain* Applications 1874/13 and 8567/13. Additionally an agreement with works council may be required.

3.2.1. Publicly available data

Publicly available personal data is information that can be obtained from the public domain.

The GDPR does not contain specific provisions regarding the personal data that can be found in the public domain. However, this does not mean that the GDPR is not applicable to such personal data. On the contrary, the same rules regarding processing of personal data apply. This also means that personal data that is publicly available, can only be processed on the basis of the same lawfulness grounds as any other personal data. Thus, such data can generally also be

⁷⁴ Rec 47

⁷⁵ *Bărbulescu v Romania*, European Court of Human Rights [2017] 61496/08

⁷⁶ Lukas Feiler and Bernhard Horn, ‘Umsetzung der DSGVO in der Praxis’ [2018] Verlag Österreich 132

⁷⁷ See for example § 96a Abs 1 Z 1 Bundesgesetz vom 14. Dezember 1973 betreffend die Arbeitsverfassung (Arbeitsverfassungsgesetz – ArbVG), BGBl. Nr. 22/1974

⁷⁸ Guidelines on Consent 7

processed on the basis of consent, however this is to be expected only in a very limited number of cases due to practicalities of this approach. Ordinarily, the processing of such personal data will be based on a different lawfulness ground.

At this point, it is important to mention that for sensitive personal data which has been evidently made public by the data subject, according to the GDPR, no explicit consent from the data subject is required.

3.2.2. Automated decision making

GDPR gives data subjects special protection against decisions based solely on automated processing, including profiling, which produces legal effects for such data subject or otherwise significantly affects them.⁷⁹ The consequence of such activity needs to be substantial enough to deserve attention and influence the individual.⁸⁰

Automated decision making is defined as the “ability to make decisions by technological means without human involvement in the decision process”.⁸¹ It is to mention that only significant human intervention would take an activity out of the definition. Such significant human involvement can only be conducted “by someone who has the appropriate authority and capability to change the decision and who will review all the relevant data including the additional elements provided by the data subject”.⁸²

Profiling means undertaking “automated processing of personal data for evaluating personal aspects, in particular to analyse or make predictions about individuals”.⁸³ Automated decision making and profiling may coincide but do not have to.

The activities described in this chapter can pose a serious risk to a data subject’s personal data. This way of processing data is not transparent and may be unintelligible for the data subject. Article 29 Working Party uses the term “opaque”.⁸⁴ Controllers may use data from different

⁷⁹ Art 22 GDPR

⁸⁰ Article 29 Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) [2017] WP258 12

⁸¹ *ibid* 11

⁸² Article 29 Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) [2017] WP258 13

⁸³ Guidelines on Automated Decision-Making and Profiling 7

⁸⁴ *ibid* 5

sources, combining data and deriving new data from the information collected with the help of modern technologies. Computer generated decisions without any human intervention may contain errors or bias.⁸⁵ Profiling may even “perpetuate existing stereotypes and social segregation.”⁸⁶ Individuals may become subject to inaccurate predictions, experience unjustified discrimination or be denied services available to others.⁸⁷

Due to such potential risks and disadvantages to the data subject, the legislator has found it necessary to implement special precautions for the use of automated individual decision making, including profiling. Therefore, such activities are prohibited unless one of the exceptions of Art 22 (2) GDPR applies. In particular, such processing can be undertaken if the data subject provides their explicit consent.⁸⁸ Explicit consent provides the data subject a stronger protection due to a high level of individual control.⁸⁹

The processes behind a decision based solely on automated processing, including profiling may be incomprehensible for a data subject, not least due to the complexity of the technologies used. The controller has the obligation to provide the data subject with “meaningful information about the logic involved”.⁹⁰ This constitutes a stronger requirement on the element of informed consent.

Data subject’s rights in respect of automated individual decision making, including profiling, do not end here. In particular, the data subject shall have the “right to obtain human intervention on the part of the controller, [...] express his or her point of view and [...] contest the decision”.⁹¹

Extra attention should be paid when special categories of data are created by profiling.⁹²

⁸⁵ Article 29 Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) [2017] WP258 13

⁸⁶ Guidelines on Automated Decision-Making and Profiling 5

⁸⁷ *ibid* 6

⁸⁸ Art 22 (2) lit c GDPR

⁸⁹ Guidelines on Automated Decision-Making and Profiling 24

⁹⁰ *ibid*

⁹¹ Art 22 (3) GDPR

⁹² Guidelines on Automated Decision-Making and Profiling 15

4. PERSONAL DATA LAW

Given the fact that the terminology of the Personal Data law differs from that of the GDPR, I decided to provide a few definitions of the main terms I'm intending to use in this chapter.

Personal data means any information which directly or indirectly belongs to an identified or identifiable natural person (personal data subject).⁹³

According to Art 3 (2) Personal Data Law, operator is “a state body, a municipal body, a legal entity, or a natural individual organizing and (or) carrying out personal data processing as well as determining the purposes and the content of personal data processing.”

Personal data processing is defined as “actions (operations) with personal data including personal data gathering, systematizing, accumulation, storage, refinement (updating, changing), use, distribution (including transmission), depersonalization, blocking, destruction of personal data”.⁹⁴

In this section, references to the law, unless otherwise indicated, shall mean the Personal Data Law.

4.1. General requirements for consent

4.1.1. Notion of consent

Consent is only one of many legal grounds for data processing specifically listed in Personal Data Law.⁹⁵ The instrument of consent shall only be used in case no other processing ground listed in Art 6 (2-11) Personal Data Law is applicable. Data processing which can be based on processing grounds listed in Art 6 (2-11) Personal Data Law does not require consent unless such consent requirement is specifically prescribed by law.⁹⁶

The instrument of consent is providing the data subject the right to decide about the processing of their personal data. This right is sourced in Art 24 of the Constitution of the Russian

⁹³ Art 3 (1) Personal Data Law

⁹⁴ Art 3 (3) Personal Data Law

⁹⁵ Art 6 (1) Personal Data Law

⁹⁶ А.А. Приезжевая, Федеральный закон «О персональных данных»: научно-практический комментарий. — М.: Редакция «Российской газеты» [2015] Вып. 11. — 176 с., page 33

Federation which states that no collection, storage, use and distribution of information concerning a personal private life shall be allowed without the subject's consent.

According to Art 9 (1) Personal Data Law, consent must be freely given, declared at the data subject's own will, and in his own interest. The consent should be specific, informed and conscious. As done earlier in this paper for the GDPR, I will break this definition down into its elements.

4.1.1.1. Freedom of consent

Freedom of consent is required, as it establishes an individual's right to make their own independent decisions regarding the use of their personal data.⁹⁷ In fact, one of the aims of the regulation of consent is to provide the data subject with the autonomy to dispose of their personal data.⁹⁸

Personal Data Law states that the data subject needs to make a decision about providing their personal data and provide consent for the processing of such data at the data subject's own will and in their own interest.⁹⁹

4.1.1.2. Specific

A specific consent means a clearly expressed and concrete permission that is particular to a certain subject and is non-abstract.¹⁰⁰ This means that the consent should be provided for instances when a specific set of personal data is to be processed in a particular way and for a particular purpose.

Only processing activities that are in-line with the defined purpose are covered by consent. If the data operator has obtained a consent for a processing activity, but such processing activity does not correspond with the identified purpose, the processing activity cannot be undertaken

⁹⁷ А.Н. Кайль и Е.А. Новиков, Комментарий к Федеральному закону от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (постатейный) [2006] Подготовлен для системы Консультант Плюс

⁹⁸ А. Савельев, Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» [2018] Статут

⁹⁹ Art 9 (1) Personal Data Law

¹⁰⁰ А.А. Приезжевая, Федеральный закон «О персональных данных»: научно-практический комментарий. — М.: Редакция «Российской газеты» [2015] Вып. 11. — 176 с., page 48

lawfully, even if the data subject has consented to such.¹⁰¹ This has for example been reflected in the judgement of the Arbitration Court of the Volga District.¹⁰²

For the data subject to be able to provide a specific consent, they need to be sufficiently informed of such processing activity. The information requirement is described in more detail during the next chapter below.

In Russia, it is generally accepted to include consent language in the body of the general terms and conditions of an agreement.¹⁰³ However, such consent should be visibly distinguishable in the agreement compared to the commercial clauses of a contract.¹⁰⁴ In this regard, the consent can be provided by ticking an un-ticked box.

4.1.1.3. Informed

Informed consent within the meaning of Art 9 (1) Personal Data Law means that the information contained in the consent document is supposed to notify the data subject about an event, fact or action and explain the intention of the same.¹⁰⁵ The data subject needs to understand the extent of the personal data being collected, purposes of data gathering and processing, sources from which personal data has been obtained, objectives and activities of data processing and have knowledge of the data operator.¹⁰⁶ In many decisions, the higher courts have pointed out the lack of explanation with regards to exactly what data processing means. However, providing the data subject with the exact language of the definition of data processing stated in Personal

¹⁰¹ А.А. Приезжевая, Федеральный закон «О персональных данных»: научно-практический комментарий. — М.: Редакция «Российской газеты» [2015] Вып. 11. — 176 с., page 48

¹⁰² Определение Арбитражного суда Поволжского округа от 4 сентября 2017 г. N Ф06-25228/17 по делу N А65-4208/2017

¹⁰³ А.А. Приезжевая, Федеральный закон «О персональных данных»: научно-практический комментарий. — М.: Редакция «Российской газеты» [2015] Вып. 11. — 176 с., page 48

¹⁰⁴ Постановление Одиннадцатого арбитражного апелляционного суда от 17.07.2017 N 11АП-8208/2017 по делу N А65-4208/2017, later confirmed by the highest court in Определение Верховного Суда РФ от 15.11.2017

¹⁰⁵ А.А. Приезжевая, Федеральный закон «О персональных данных»: научно-практический комментарий. — М.: Редакция «Российской газеты» [2015] Вып. 11. — 176 с., page 48

¹⁰⁶ Постановление Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" // Собр. законодательства РФ. - 22 сентября 2008 г. N 38 ст. 4320

Data Law without going into details of the actual processing operations would seem to suffice here.¹⁰⁷

The data subject also needs to be informed of their right to withdraw the consent and the modalities of such withdrawal. Withdrawal of consent is discussed in more detail during Chapter 4.1.2 below.

Art 9 (4) Personal Data Law provides a list of information that needs to be present in a written consent document. These requirements will be described in more detail during chapter **Fehler! Verweisquelle konnte nicht gefunden werden.** Form requirements.

The requirements of an informed consent are directly linked to the Constitution of the Russian Federation. Art 24 of the Constitution states that the data subject shall have the right to make himself familiar with documents and materials, directly affecting his rights and freedoms.¹⁰⁸

4.1.1.4. Conscious

As defined by Priezzhaevaya in her Commentary to the law,¹⁰⁹ a conscious consent means a meaningful, thought through and sensible decision.

This criterion is strongly tied to the requirement of informed consent. An individual can only make a conscious decision if they have a good understanding of the modalities of data processing. The Eleventh Arbitral Appeal Court has therefore clarified in its decision of 17 July 2017, that a consent can only be specific, informed and conscious if the data subject has at least been explained the concept of “personal data processing” in writing.¹¹⁰ As stated above, providing the legal definition of data processing contained in Art 3 (3) Personal Data Law seems to satisfy the courts in this respect.

¹⁰⁷ Постановление Одиннадцатого арбитражного апелляционного суда от 17.07.2017 N 11АП-8208/2017 по делу N А65-4208/2017; Постановление Арбитражного суда Северо-Западного округа от 18 июля 2016 г. N Ф07-5537/2016 по делу N А44-9647/2015

¹⁰⁸ Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 года. : (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ30 декабря 2008 № 6-ФКЗ и № 8 – ФКЗ) // Собр. законодательства РФ. - 2014. - № 31 - Ст. 4398 (**Constitution of the Russian Federation**) // Art 24

¹⁰⁹ А.А. Приезжевая, Федеральный закон «О персональных данных»: научно-практический комментарий. — М.: Редакция «Российской газеты» [2015] Вып. 11. — 176 с., page 48

¹¹⁰ Постановление Одиннадцатого арбитражного апелляционного суда от 17.07.2017 N 11АП-8208/2017 по делу N А65-4208/2017, later confirmed by the highest court in Определение Верховного Суда РФ от 15.11.2017 N 306-АД17-1652

4.1.1.5. Act of consent

According to Art 9 (1) Personal Data Law, consent can be given in any form that allows the controller to confirm the receipt of such consent.

Companies are required to have templates for a consent document, as well as an informative document notifying the data subject about the consequences of not providing their personal data to such a company.¹¹¹

4.1.1.6. Written consent

In many cases, the law prescribes the consent to be written. As stated in Art 9 (4), this criterion can be fulfilled either by a hard copy document with the data subject's signature or an electronic signature as defined in the Federal law on electronic signatures.¹¹² The written consent form needs to include a possibility of the data subject confirming their intention by setting an action in motion, which cannot be set automatically.¹¹³ This excludes the possibility of using pre-ticked boxes.

Such written consent should include inter alia company name or first name, last name, patronymic and address of the data operator who is receiving the consent to process personal data. The first name, last name, patronymic and address of the data subject also needs to be present along with the purpose of processing, list of personal data to be processed, list of processing activities and period of time for which the consent is given.¹¹⁴ It is important to note that this provision may require the data subject to provide more personal data within the consent than will actually be necessary for the processing itself.

¹¹¹ Постановление Правительства РФ от 21.03.2012 N 211 (ред. от 06.09.2014) "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" // Первоначальный текст документа опубликован в Собр. законодательства РФ. - 02 апреля 2012 г. N 14 ст. 1626

¹¹² Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) "Об электронной подписи": принят Гос. Думой Федер. Собр. Рос. Федерации 25 марта 2011 г.: одоб. Советом Федерации Федер. Собр. Рос. Федерации 30 марта 2011 г. (с изм. и доп., вступ. в силу с 31.12.2017) // Собр. законодательства РФ. - 11 апреля 2011 г. N 15 ст. 2036

¹¹³ Постановление Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" // Собр. законодательства РФ. - 22 сентября 2008 г. N 38 ст. 4320

¹¹⁴ Art 9 (4) Personal Data Law

In particular, written consent is required for processing of sensitive data,¹¹⁵ to transfer personal data to countries with no adequate protection (even if the data is transferred within a single group of companies),¹¹⁶ for automated decision making and profiling¹¹⁷ and when publishing personal data in public sources.¹¹⁸

4.1.1.7. Obligation to demonstrate consent

As mentioned in chapter 4.1.1.5 above, the data operator has a duty to prove that the data subject has consented to processing activities undertaken by the data operator. Such proof can be provided by the data operator in the form of a written consent or in any other form which is suitable to prove the data subject's consent.¹¹⁹ According to the Code of Civil Procedure of the Russian Federation such proof can be any information received by the court in accordance with the correct legal procedure on the basis of which the court establishes presence or absence of the circumstances that justify the claims or defenses of the parties.¹²⁰

4.1.2. Withdrawal of consent

The data subject has the right to withdraw the consent at any time in accordance with Art 9 (1) Personal Data Law. However, it is important to note that Art 9 (2) Personal Data Law states that in certain cases the data operator may continue processing the data after such withdrawal.

According to Art 21 (5), the operator should cease the processing of personal data and delete or destroy the personal data if it is no longer required for the purposes of data processing. This needs to be within 30 days from the data subject's request. The controller does not need to notify the data subject about having stopped processing the data.¹²¹

¹¹⁵ Art 10 (2) 1 Personal Data Law

¹¹⁶ Art 12 (4) 1 Personal Data Law

¹¹⁷ Art 16 (2) Personal Data Law; see also Chapter 4.2.4 below

¹¹⁸ Art 8 (1) Personal Data Law

¹¹⁹ Art 9 (3) Personal Data Law

¹²⁰ "Гражданский процессуальный кодекс Российской Федерации" от 14.11.2002 N 138-ФЗ (ред. от 02.12.2019) (с изм. и доп., вступ. в силу с 30.03.2020): принят Гос. Думой Федер. Собр. Рос. Федерации 23 октября 2002 г.; одобрен Советом Федерации Федер. Собр. Рос. Федерации 30 октября 2002 г. // Собр. законодательства РФ. - 18 ноября 2002 г. N 46 ст. 4532

¹²¹ Приезжева А.А. Федеральный закон «О персональных данных»: научно-практический комментарий. — М.: Редакция «Российской газеты», 2015, Вып. 11. — 176 с., page 49

Personal Data Law does not specify any form requirements for the withdrawal of consent. The data subject needs to be informed of his right to withdraw their consent and the modalities of how a consent can be withdrawn.¹²²

Priezzhaevaya continues to mention in her commentary that only a consent can be provided by a representative, not its withdrawal.¹²³ However, there is no reason to justify this assumption. The legal representative or a person holding the appropriate power of attorney shall have the right to withdraw data subject's consent. The latter view has also been expressed by Amelin and others in their commentary to the law.¹²⁴

4.1.3. Time limit for consent

If processing of personal data is based on consent, such consent is given for a certain period of time. This time period needs to be named in the consent document in accordance with Art 9 (4) 8 Personal Data Law. In practice, the consent is given for 75 years.

It is, however, to mention that according to Art 5 (7) Personal Data Law, storage of personal data in a way that allows the identification of the data subject should be allowed, only so long as required for the legitimate purposes of data processing, unless a limitation in time is set out by a federal law or contract to which data subject is a beneficiary, party or guarantor.

4.1.4. Consent by representative

Art 9 (1) states that the consent can be given by the data subject or their representative. In line with Priezzhaevaya's interpretation,¹²⁵ this means that the data subject can issue a power of attorney providing a different individual with the right to consent to data processing on their behalf. In this case the general rules on powers of attorney need to be followed.¹²⁶ In case of

¹²² А.Н. Кайль и Е.А. Новиков, Комментарий к Федеральному закону от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (постатейный) [2006] Подготовлен для системы Консультант Плюс

¹²³ Приезжевая А.А. Федеральный закон «О персональных данных»: научно-практический комментарий. — М.: Редакция «Российской газеты», 2015, Вып. 11. — 176 с., page 49

¹²⁴ Р.В. Амелин и др. ,Комментарий К Федеральному Закону От 27.07.2006 N 152-ФЗ "О Персональных Данных"“ [2013] Подготовлен для системы КонсультантПлюс

¹²⁵ Приезжевая А.А. Федеральный закон «О персональных данных»: научно-практический комментарий. — М.: Редакция «Российской газеты», 2015, Вып. 11. — 176 с., page 49

¹²⁶ Часть первая Гражданского кодекса Российской Федерации от 30 ноября 1994 г. N 51-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 21 октября 1994 г. // Собр. законодательства РФ. – 1994. - № 32 ст. 3301 (**Russian Civil Code**) // Art 185-186

the data subject's legal incapacity, the consent to process the data subject's data can be given by his legal representative.

Rules regarding providing consent for a minor by a parent or legal guardian are described in Chapter 4.2.1 below.

4.2. Specific circumstances for consent

Like the GDPR, Personal Data Law has put in place certain rules for processing of personal data in specific circumstances. Such circumstances are discussed in more detail below.

4.2.1. Consent provisions for children

The current law does not contain any special provisions regarding the processing of personal data of minors. A draft law was proposed in November 2017 and is currently being reviewed by the State Duma to include special provisions regarding the processing of minors' data.¹²⁷ In accordance with its suggested wording, consent for the processing of a minor's personal data should be given by their parent or guardian. A data subject over the age of 16 should have the right to consent to a processing activity in case such activity is being undertaken in connection to such minor's employment. Furthermore, personal data of minors should be added to the list of special categories of data in Art 10 Personal Data Law and shall be treated as such.

However, in the absence of any currently valid specific provisions for consent to processing of personal data of minors, the processing of such data is regulated by the general provisions of Personal Data Law as well as the provisions of the civil law.

According to the Art 21 (1) Civil Code of the Russian Federation, the adulthood is reached at the age of 18, unless a minor reaches the full civil capacity earlier.¹²⁸ Art 9 (6) Personal Data Law enables a representative to consent in case of data subject's incapacity which can be applied to minors until the age of 14.

Minors from the age of 14 to 18 can only perform certain activities listed in Art 26 (1) Civil Code of the Russian Federation without their legal representative's consent. It is not clear whether this also enables them to consent to processing of their personal data. Because of this

¹²⁷ Законопроект № 305068-7 О внесении изменений в Федеральный закон "О персональных данных" <[http://asozd2.duma.gov.ru/main.nsf/\(Spravka\)?OpenAgent&RN=305068-7](http://asozd2.duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=305068-7)> accessed 6 April 2020 (**Draft Law**)

¹²⁸ Art 27 (1) Russian Civil Code

legal uncertainty of such situations it is often recommended to obtain a consent of both the minor with limited legal capacity as well as their parent or guardian.¹²⁹

For reasons of completion it is to mention that according to a dissenting opinion, consent for any person who has not reached adulthood should be provided by their parent or legal guardian.¹³⁰

4.2.2. Data processing in the workplace

According to the Art 86 (1) Labour Code of the Russian Federation,¹³¹ an employer can process its employee's personal data if such processing is required in order to:

ensure compliance with the laws and other regulatory acts, provide assistance in searching for employment, for educational reasons or reasons of career development, to ensure employees' personal safety and to ensure the quality and quantity of work as well as preservation of property.

Employers do not require employees' consent if the data processing activity is mandatory by law. Likewise, no consent is required if a processing activity is prescribed by collective agreement, internal work regulations, as well as local regulations adopted by the employer according to the procedure prescribed in Art 372 Labour Code.¹³²

For example, this is the case for legal requirements to transfer personal data to the Russian Social Insurance Fund, Pension Fund,¹³³ etc. However, when a transfer of data to a third party is not compulsory by law, a written consent from the data subject is needed. This includes transfer of data to third parties, like providers of human resources and accounting services, tax

¹²⁹ Федеральная служба по труду и занятости, Консультация эксперта, „Вопрос: Кто должен давать работодателю согласие на обработку персональных данных несовершеннолетнего работника, работающего в свободное от получения образования время?“ [2017]

¹³⁰ Р.В. Амелин и др. „Комментарий К Федеральному Закону От 27.07.2006 N 152-ФЗ "О Персональных Данных"" [2013] Подготовлен для системы КонсультантПлюс

¹³¹ Трудовой кодекс Российской Федерации от 30 декабря 2001 г. N 197-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 21 декабря 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 26 декабря 2001 г. // Собр. законодательства РФ. – 2002. - № 1 (часть I) ст. 3 (**Russian Labour Code**)

¹³² Министерство Связи И Массовых Коммуникаций Российской Федерации, Федеральная Служба По Надзору В Сфере Связи, Информационных Технологий И Массовых Коммуникаций, „Разъяснения „Вопросы, Касающиеся Обработки Персональных Данных Работников, Соискателей На Замещение Вакантных Должностей, А Также Лиц, Находящихся В Кадровом Резерве““ // Подготовлен для системы Консультант Плюс // <http://www.consultant.ru/document/cons_doc_LAW_139574/> accessed on 10 April 2020

¹³³ Art 22 Russian Labour Law

advisors, but also banks, insurance companies and even companies affiliated with the employer. The latter case includes placing personal data on the intranet site of a group of companies.

According to Art 88 Labour Law, data operators or third parties who have access to personal data are obliged to keep the data confidential and to not disseminate it without the data subject's written consent, except when such transfer is necessary to prevent a risk to life and / or health of the employee.

Written consent, as it is described in section **Fehler! Verweisquelle konnte nicht gefunden werden.**, is also required when obtaining personal data of a data subject from a third party¹³⁴ and disseminating employee's personal data for commercial reasons.¹³⁵ The latter applies if the employer wishes to include employee's contact information or other personal data into address books or place it on the company's website.

The employer may also process the health data of an employee. Unless such processing is legally required for purposes of mandatory medical checks, control of sick leave or other compulsory requirements, the employer needs to rely on the written consent of the employee, as health data is included in the special categories of data.

Employee's consent under Russian legislation can either be contained in the employment agreement or be signed as a separate document. In case employee's personal data is processed without their consent, the employee has the right to demand explanation from the employer.¹³⁶

For reasons of completion, it should be noted that civil servants have special provisions regarding the processing of their personal data by their employer.¹³⁷ However, in terms of the consent requirements, these provisions do not differ from the provisions set out by Section 14 of the Labour Code of the Russian Federation.

¹³⁴ А.Н. Кайль и Е.А. Новиков, Комментарий к Федеральному закону от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (постатейный) [2006] Подготовлен для системы Консультант Плюс

¹³⁵ Art 88 Russian Labour Law

¹³⁶ А.Н. Кайль и Е.А. Новиков, Комментарий к Федеральному закону от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (постатейный) [2006] Подготовлен для системы Консультант Плюс

¹³⁷ Федеральный закон "О государственной гражданской службе Российской Федерации" от 27.07.2004 N 79-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 7 июля 2004 г.: одоб. Советом Федерации Федер. Собр. Рос. Федерации 15 июля 2004 г. // Собр. законодательства РФ. – 2004. – N 31 ст. 3215 // глава 7

Fully automated decisions concerning employee's interests are prohibited, even if the data subject would consent to such.¹³⁸

4.2.2.1. Recruiting process

The processing of a job applicant's personal data is subject to the candidate's consent. In these cases, the consent is given for the period of time needed in order for the potential employer to decide whether to hire the candidate. If a candidate is unsuccessful in obtaining employment, the data operator shall return, delete or destroy the applicant's data within 30 days, unless a different retention period is required by law.¹³⁹

Roskomnadzor¹⁴⁰ has clarified that the candidate's consent is not required if the candidate has made his curriculum vitae publicly accessible online or in case the information has been obtained from a recruiting company with which the candidate has signed an agreement.¹⁴¹

Any processing activity that goes beyond the consideration of the candidate for the particular job offering such candidate applied to, requires separate consent. Thus, the potential employer needs to obtain consent for requesting references on the candidate from third parties, as well as for including the candidate in a personnel reserve, unless such activity is obligatory by law. This can be the case for public servants.¹⁴²

4.2.2.2. Background Checks

The Labour Code of the Russian Federation prescribes certain mandatory checks. In this way, mandatory medical or criminal checks for certain professions do not require the data subject's

¹³⁸ Art 86 (6) Russian Labour Law

¹³⁹ Such as for example provided by law for civil servants. In this case the job applications need to be kept for a period of 3 years.

¹⁴⁰ Federal Service for the Supervision of Communications, Information Technology and Mass Communications (**Roskomnadzor**)

¹⁴¹ Министерство Связи И Массовых Коммуникаций Российской Федерации, Федеральная Служба По Надзору В Сфере Связи, Информационных Технологий И Массовых Коммуникаций, „Разъяснения „Вопросы, Касающиеся Обработки Персональных Данных Работников, Соискателей На Замещение Вакантных Должностей, А Также Лиц, Находящихся В Кадровом Резерве““ // Подготовлен для системы Консультант Плюс // <http://www.consultant.ru/document/cons_doc_LAW_139574/> accessed on 10 April 2020

¹⁴² eg Art 61 (1) Russian Labour Code of the Russian Federation

consent. Same applies for running a candidate's name against the database of disqualified personnel.¹⁴³

For any additional background checks of a potential or current employee, the company will require prior written consent from the data subject. Undertaking background checks is a common practice in the Russian Federation.

4.2.2.3. E-mails and device monitoring

Monitoring of e-mails, phone conversations and employee's devices should only be possible upon such employee's prior consent. Aforesaid monitoring can only be put in place in respect of devices that are owned by the employer and provided to the employee for work purposes. Personal use of such devices should be prohibited in employer's internal regulations.

4.2.2.4. CCTV

In accordance with Art 74 Labour Code of the Russian Federation, an employer has the right to implement a CCTV system for the purposes of recording possible unlawful activities. Should the employer make use of such rights, the employees must be notified of such a change in their working environment and provide a signature signifying their acknowledgement of the change. This is the case due to the fact that such implementation is regarded as a significant change of the employment agreement. Visitors of premises that are subject to video surveillance need to be notified of the possible recording upon entry. No consent within the meaning of Art 9 Personal Data Law is required.

Surprisingly, the Ministry of Labour of the Russian Federation went as far as to say that an employee disagreeing with the implementation of the CCTV systems may have their employment contract terminated.¹⁴⁴

¹⁴³ Database of disqualified personnel is publicly available under <<https://service.nalog.ru/disqualified.do>> accessed 6 April 2020

¹⁴⁴ Консультация эксперта, Минтруд России, „Можно ли уволить работников, которые не согласны на установку системы видеонаблюдения, и в каком порядке?“ [2018] <<http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=QUEST002;n=176425#08835337009240061>> accessed 6 April 2020

According to the clarification of Roskomnadzor,¹⁴⁵ as long as the picture or video material is not used for identifying a data subject, Personal Data Law does not apply.¹⁴⁶ Data recorded by CCTV and used for purposes of identifying a data subject is regarded as biometric data. For processing of such data, the data operator requires written consent, unless one of the exceptions of Art 11 (2) Personal Data Law applies.

4.2.3. Publicly available data

Processing of publicly available personal data is allowed if such data is accessible to an unlimited number of persons and it had been either made public by the individual themselves or on their behalf.¹⁴⁷ Due to the first criteria, publicly available data can only be contained in publicly available sources. Such publicly available sources should be created in accordance with Art 8 Personal Data Law. In particular, this includes phone and address books. Furthermore, Art 8 details what data can be included in a public directory about a data subject, upon such data subject's consent.

It has been previously clarified that without a data subject's written consent, it is not possible for the data operator to rely on the fact that the information had been made public by the data subject himself. The obligation of providing a proof that the data subject's consent to the processing of their personal data has been obtained is imposed on the operator.¹⁴⁸ Same applies for personal data contained in public sources. In this case the operator must prove that personal data has been obtained from a public source.

It is important to point out that data made public by a data subject on their social media account/s is not considered to be publicly accessible data within the meaning of Art 6 (10) Personal Data Law, as a social media site does not fulfil the criteria of being a publicly available

¹⁴⁵ Federal Service for the Supervision of Communications, Information Technology and Mass Communications (**Roskomnadzor**)

¹⁴⁶ Федеральная Служба По Надзору В Сфере Связи, Информационных Технологий И Массовых Коммуникаций, „Разъяснения „О Вопросах Отнесения Фото- И Видео- Изображения, Дактилоскопических Данных И Иной Информации К Биометрическим Персональным Данным И Особенности Их Обработки““ [2013] < <https://pd.rkn.gov.ru/press-service/subject1/news2729/>> accessed 6 April 2020

¹⁴⁷ Art 6 (10) Personal Data Law

¹⁴⁸ Art 9 (3) Personal Data Law

source described in Art 8 (1) Personal Data Law.¹⁴⁹ This view has subsequently been confirmed by higher courts, including the Supreme Court of the Russian Federation.¹⁵⁰

In accordance with Art 10 (2) 2 Personal Data Law, a data operator may even process special categories of data if such information had been made publicly accessible by the data subject.

4.2.4. Automated decision making

According to Art 16 (1) Personal Data Law, it is prohibited to take decisions that have legal consequences for a data subject or otherwise affect their rights and lawful interests based solely on automated processing of personal data. Automated decision-making is defined by the lack of human intervention in the decision-making process.¹⁵¹

According to Art 16 (2) Personal Data Law, the data operator can base his decisions solely on automated processing if the data subject had provided a written consent to such processing. In addition to the above, the data operator has the obligation to explain the modalities of automated decision-making to the data subject and disclose potential legal consequences of such automated decision, provide the possibility to make an objection to such decision and inform the data subject of his rights and legal interests in respect of such decision.¹⁵²

As mentioned before during Chapter 4.2.2, automated decision making cannot be used in employment environment.

¹⁴⁹ Решение Арбитражного суда города Москвы от 5 мая 2017 года по делу № А40-5250/17-144-51

¹⁵⁰ Определение Верховного Суда РФ от 29.01.2018 N 305-КГ17-21291 по делу N А40-5250/2017

¹⁵¹ Р.В. Амелин и др. „Комментарий К Федеральному Закону От 27.07.2006 N 152-ФЗ "О Персональных Данных"“ [2013] Подготовлен для системы КонсультантПлюс

¹⁵² Art 16 (3) Personal Data Law

5. COMPARISON

As defined in section 2 Method above, I decided to undertake my research by defining a common point of reference to which I could compare the provisions described in Sections 3 GDPR and **Fehler! Verweisquelle konnte nicht gefunden werden.** Personal Data Law above. For the purposes of this research, I assume that the laws described above are solving the issue of obtaining a valid representation of individual's wishes regarding the processing of their own personal data.

The first characteristic to be compared is the notion of consent, as well as the definition of each of its elements. Then I will be looking at consent in specific circumstances.

GDPR and Personal Data Law use different terminology for comparable constructs. For the purposes of this master thesis and for better readability during this chapter, I will introduce common terminology for such constructs.

For the purposes of this chapter, I will refer to the “data controller” as defined by the GDPR¹⁵³ and the “data operator” of the Personal Data Law¹⁵⁴ as “processing entity”. The term “data subject” will be used to describe the individual whose personal data is being processed. In the interest of simplicity and clarity, “personal data” will be used as a blanket term regardless of potential differences in the definition of this term in GDPR and Personal Data Law.

5.1. General requirements for consent

5.1.1. Notion of consent

The basic concept of consent in Personal Data Law and the GDPR originates from the same underlying idea: the objective of giving the data subject freedom to decide about the processing of their data as they see fit.

According to the GDPR, as well as Personal Data Law, processing can only occur if the processing entity has a legal ground for such action. Each law provides an exhaustive list of

¹⁵³ Art 4 (7) GDPR

¹⁵⁴ Art 3 (2) Personal Data Law

such processing grounds.¹⁵⁵ Only if no other processing ground can be used, a processing entity should rely on consent.¹⁵⁶

By making consent the weakest of the processing grounds, the lawmakers ensured that unless processing is deemed necessary by law (and therefore corresponds with one of the other processing grounds), no entity shall have the right to use a data subject's data without the agreement of the latter. In this way, the data subject's control over their personal data is ensured. As discussed before, in both jurisdictions the concept of consent can be closely linked to the human right of privacy.

The elements of consent vary in both jurisdictions regarding their definition, as well as in their application. Therefore, it makes sense to look at them one at a time. In order to undertake an effective comparison, the elements of consent of the General Data Protection Regulation have been grouped with their closest counterparts in the Personal Data Law.

5.1.1.1. Freedom of consent

Both the GDPR and the Personal Data Law state that consent should be free. However, looking at these requirements in detail shows fundamental differences in the meaning and practical consequences of a free consent.

Art 9 (1) Personal Data Law sets out that consent should manifest the data subject's own will and interest. Such criterion is not present in the GDPR. For the data subject's "own will and interest" and therefore their intention to be taken into account by the law, could signify a possible advantage for the data subject. However, unfortunately this element does not seem to be significant in court practice. Instead of providing the individual a genuine choice, which is strived for by the GDPR (and confirmed by several opinions and interpretations of the law), the requirement of Art 9 (1) Personal Data Law seems to be of pure bureaucratic nature.

A source of insight into this matter is given by a decision of the Eleventh Arbitral Appeal Court of the Russian Federation in 2017.¹⁵⁷ In this decision, the court had criticized a processing entity for disregarding the element of freedom of consent. The agreement signed with a bank by the

¹⁵⁵ Art 6 (1) GDPR; Art 6 (1) Personal Data Law

¹⁵⁶ Art 6 (2) Personal Data Law; Article 29 Working Party, Opinion 15/2011 on the definition of consent [2011] WP187 (**Opinion on the Definition of Consent**)¹⁰

¹⁵⁷ Постановление Одиннадцатого арбитражного апелляционного суда от 15.01.2018 N 11АП-17453/2017 по делу N А65-25979/2017

data subject contained a pre-ticked box next to the privacy clauses. By signing the agreement for the provision of services, the data subject had also been consenting to their data being processed by the bank. In the court's opinion the box should have been un-ticked. The data subject would then instead be able to demonstrate their own will and interest by ticking the box themselves. The above means, that in the practical application of the criterion, the courts are not looking for the data subject's inner intention to dispose of their data, but rather whether an appropriate action by the data subject had been set. Under the GDPR, the discussion regarding ticking un-ticked boxes falls into the criterion of specificity and/or unambiguity of consent but does not affect the criterion of the freedom of consent.

Another big difference in the application of consent crystalizes when looking at when a processing entity can actually rely on consent. In a different decision of the Eleventh Arbitral Appeal court¹⁵⁸, an insurance agency claimed that consent to process their personal data had been given by the data subject because the data subject had signed an insurance agreement. The court has ruled that the consent of the data subject in this case is invalid, as it is not free. In the court's opinion, consent should have been given as a separate written declaration fulfilling the requirements of informed consent. The court further referred to the fact that providing consent by signing the insurance agreement is impossible, as the insurance agreement does not provide for an alternative, i.e. the agreement does not offer the possibility of not providing personal data.

If a comparable case would be reviewed under the GDPR, the processing entity would not have a possibility to use legal ground of consent for this processing activity. Consent being the weakest legal ground, it can only be used if no other processing grounds are applicable. In the case of the insurance agreement at hand, the processing entity would be able to process the data which is necessary for the fulfilment of the agreement in accordance with Art 6 (1) lit b GDPR.

Article 29 Working Party stresses that the term "necessary for the performance of the contract" should be interpreted strictly.¹⁵⁹ It further states that "[c]ompulsion to agree with the use of personal data additional to what is strictly necessary limits data subject's choices and stands in

¹⁵⁸ Постановление Одиннадцатого арбитражного апелляционного суда от 17.07.2017 N 11АП-8208/2017 по делу N А65-4208/2017, later confirmed by the highest court in Определение Верховного Суда РФ от 15.11.2017

¹⁵⁹ Article 29 Working Party, Guidelines on consent under Regulation 2016/679 [2017] revised in 2018 (**Guidelines on Consent**) 9

the way of free consent”.¹⁶⁰ There therefore needs to be a strict separation of processing activities necessary for the performance of the service or to take steps at the request of the data subject prior to entering into a contract and data processed for a different purpose. If any additional data, other than the data necessary for the delivery of the services, is the requested the processing entity should additionally require consent for processing of such data. However, in this case the data subject should have the possibility to deny their consent without negative consequences. This means that the insurance agency could not make the consent for the additional data processing (e.g. for direct marketing purposes) a precondition to the provision of insurance services.

In the decision at hand, the Russian court does not indicate that the performance of the insurance agreement is not possible without processing of data. Obtaining the consent from the individual in this case makes consent a precondition to the insurance agreement and therefore would undermine its freedom, had it been reviewed based on the provisions of GDPR, as the individual has to agree to the processing of his data if they wish to obtain insurance services.

In fact, in its decision № 2-3512/2014 the Court of the City of Psov has indicated that services (in this case medical services) can be provided irrespective of data subject’s consent to use their personal data, since the processing entity can rely on a different processing ground to process such data.¹⁶¹

During my research, I also noticed a fundamentally different approach regarding consent in an employment environment. Whilst under the GDPR the processing entity is generally not able to rely on consent and the request of providing consent by its employees could be regarded as “misleading and inherently unfair”,¹⁶² under the Personal Data Law, provision of consent by the employee of the processing entity is a common practice. This particular subject matter is discussed in chapter 5.2.3.

To summarise, both EU and Russian legislation identify the requirement of consent freedom. However, the practical application of this requirement differs substantially. Under the GDPR, consent can only be provided and valid if such constitutes a genuine choice, whereas under

¹⁶⁰ *ibid* 8

¹⁶¹ Решение Псковского городского суда Псковской области от 30 октября 2014 г. по делу № 2-3512/2014

¹⁶² Article 29 Working Party, Opinion 15/2011 on the definition of consent [2011] WP187 (**Opinion on the Definition of Consent**) 13

Russian legislation, a consent is free if the data subject has been informed of the consequences of the consent and has set about an unambiguous act accepting the provision, irrespective of the data subject's ability to make a decision.

This difference is consistent with the legislator's view that a data subject may be required to provide consent even if this contradicts their potential choice.¹⁶³

The freedom of consent does not only include the freedom of giving consent, but also the freedom of withdrawing the consent at any time. Both jurisdictions honour this right. A comprehensive review of the mechanism of withdrawal is contained in chapter 5.1.2.

5.1.1.2. Specific

Both jurisdictions require the consent to be specific. This means that the consent cannot be provided as a general permission to process data, but instead the data subject needs to agree to specific processing activities to be undertaken in respect of a defined set of personal data for a particular purpose.

Both jurisdictions set strong requirements regarding the identification of the purpose for processing. GDPR considers a consent only to be lawful if the individual has consented to processing activities that are "reasonable and necessary in relation to the purpose".¹⁶⁴ Russian legal practice follows a similar interpretation. Thereafter, a processing entity should not be obtaining consent for an excessive list of processing activities, without clearly referencing them to a particular purpose.¹⁶⁵ In fact, as mentioned before in chapter 4.1.1.2, under Personal Data Law a consent obtained for a processing activity that does not correspond with the defined purpose, will be invalid.

Like in the GDPR, the consent under Art 9 Personal Data Law has to be given for a certain processing activity. In case the entity processing personal data wishes to use data already obtained for a purpose different to the one for which the consent was given, and no other lawfulness grounds for processing of such information apply, the entity is required to obtain a new consent for each new processing activity.

¹⁶³ Art 9 (2) Personal Data Law

¹⁶⁴ Opinion on the Definition of Consent 17

¹⁶⁵ See Определение Арбитражного суда Поволжского округа от 4 сентября 2017 г. N Ф06-25228/17 по делу N A65-4208/2017

Under the GDPR, the above requirement is reinforced by the principle of granularity, according to which the individual should be able to consent to different processing activities individually.¹⁶⁶ While Personal Data Law requires all processing activities to be listed, it does not provide the data subject with the right to pick-and-choose the processing activities one is consenting to.

The specificity requirement in both jurisdictions is closely tied with the information requirement, as the data subject can only provide a consent to processing activities when such are defined at the time of consent.

When including the consent provisions into the body of an agreement or general terms and conditions, Personal Data Law as well as GDPR require the provision of consent to be unambiguous and separate from the acknowledgement of other terms.¹⁶⁷

One element of specific consent under the Personal Data Law is the requirement of the consent being clearly expressed. This requirement will be discussed in chapter 5.1.1.4 below, which reviews the requirement of unambiguity.

5.1.1.3. Informed

The laws are consistent in their requirement that the data subject should be provided with certain information at the time of consent.

Unsurprisingly, in both jurisdictions the data subject is expected to understand the extent to which their data is collected and processed, the purpose of each processing activity and the identity of the entity processing the data. Data subjects are also expected to have access to information about their rights in respect of the data processed, in particular, the right to withdraw consent.¹⁶⁸

Additional information requirements are necessary according to the GDPR in case of automated decision-making¹⁶⁹ or data transfers into countries that do not have an adequate level of

¹⁶⁶ Rec 43 GDPR

¹⁶⁷ Постановление Одиннадцатого арбитражного апелляционного суда от 17.07.2017 N 11АП-8208/2017 по делу N А65-4208/2017; Art 7 (2) GDPR

¹⁶⁸ Guidelines on Consent 13; А.Н. Кайль и Е.А. Новиков, Комментарий к Федеральному закону от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (постатейный) [2006] Подготовлен для системы Консультант Плюс

¹⁶⁹ See Chapter 3.2.2 Automated decision making

protection.¹⁷⁰ Under Personal Data Law, in such and other cases, the entity processing personal data is supposed to seek written consent from the data subject and therefore provide information necessary to obtain written consent in accordance with Art 9 (4) Personal Data Law.¹⁷¹ In practice, most consent under the Personal Data Law is required to be in written format. The Personal Data Law has undeniably stronger requirements for an “informed consent” if a written consent is required by law.¹⁷²

GDPR requires the consent to be understandable for the data subject.¹⁷³ The Personal Data Law lacks such provision. However, courts tend to be on the side of the data subject in cases where the consent language is not sufficiently clear and transparent. The Eleventh Arbitration Court of Appeals has often found the data subject to be not sufficiently informed, as the consent language was within the general terms and conditions document, printed in very small font and using wording that is specific to the language of the Personal Data Law and not used in day-to-day conversations.¹⁷⁴

5.1.1.4. Unambiguous

The requirement of unambiguity only exists in the GDPR. It includes a clear action of the data subject that unmistakably shows the intention to consent and the ability of the processing entity to prove that such action was performed.

Even though Personal Data Law does not mention that the consent has to be unambiguous, this requirement exists within the understanding of other provisions of the law. Therefore, requirement of a specific consent under the Personal Data law contains the need for consent to be clearly expressed and concrete.¹⁷⁵

In their commentary, Kail and Novikov have clarified that personal data may only be processed if the data subject has unambiguously provided their consent.¹⁷⁶ Russian legislation requires the

¹⁷⁰ Art 49 (1) a GDPR

¹⁷¹ See Chapter 5.1.1.7 Reinforced consent

¹⁷² Art 9 (4) Personal Data Law; see **Fehler! Verweisquelle konnte nicht gefunden werden.** above

¹⁷³ Art 7 (2) GDPR

¹⁷⁴ Постановление Одиннадцатого арбитражного апелляционного суда от 17.07.2017 N 11АП-8208/2017 по делу N А65-4208/2017

¹⁷⁵ See 4.1.1.2 above

¹⁷⁶ А.Н. Кайль и Е.А. Новиков, Комментарий к Федеральному закону от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (постатейный) [2006] Подготовлен для системы Консультант Плюс

consent to be either provided in written form or any other verifiable form.¹⁷⁷ This is consistent with the GDPR, according to which the controller should be able to clearly demonstrate consent.

As already mentioned in chapter 5.1.1.2 on specific consent, both Personal Data Law and GDPR require consent to be clearly distinguishable from other terms and conditions, even if such are contained in the same document. In addition, the act of consenting needs to be a separate action to the act of agreeing to the rest of the terms and conditions (e.g. separate signature, ticking an un-ticked box).

5.1.1.5. Conscious

Even though under the requirement of consciousness of Personal Data Law, literature may understand a rational thought through decision of the data subject, in practice this criterion shows to be a reinforcement of the consent to be informed and specific. As mentioned before, the consent signifying the free will of the data subject is questionable as in many given examples, the data subject does not have a genuine choice.¹⁷⁸

This criterion does not add to the understanding of consent in the Personal Data Law and is rarely subject to a dispute. Therefore, a lack of this element in the GDPR does not have influence on the comparison or in fact practical implications of consent.

5.1.1.6. Act of consent

Unless a written consent is required, Personal Data Law accepts any form of consent so long as the controller can demonstrate that such consent was given.¹⁷⁹ In this regard, the laws are very similar as the GDPR doesn't require a specific form to provide consent while requiring the processing entity to prove that such was given.

¹⁷⁷ Art 9 (1) Personal Data Law

¹⁷⁸ See also chapter 5.1.1.1 Freedom of consent

¹⁷⁹ See also chapter 5.1.1.8. Duty to demonstrate consent

As indicated earlier, neither law allows the use of pre-ticked boxes or other forms of consent provided by inactivity (e.g. not replying to an e-mail). This is also reflected in the current judicature of Russian courts¹⁸⁰ as well as on the European level.¹⁸¹

5.1.1.7. Reinforced consent

It is clearly visible that both laws consider the processing of certain categories of data and certain processing activities as high risk and therefore put stronger requirements on the validity of consent. This is for example the case when special categories of personal data are being processed, in the event of automated decision making and transferal of personal data to countries with legal systems that are considered as providing insufficient protection for personal data by the relevant government body. For these cases, Personal Data Law requires written consent from the data subject,¹⁸² while the GDPR calls for an explicit consent.¹⁸³

In cases where the Personal Data Law stipulates a written consent, the law provides for a list of information to be included in such consent document. If the list is incomplete, the data subject's consent is not considered valid.¹⁸⁴ GDPR does not have a comparable form requirement. As mentioned above in chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**, the written consent may require the data subject to provide more information than needed for the processing. For the processing of personal data that is only provided for the purposes of the written consent, an additional consent is not required. Within the GDPR, the principle of data minimization comes into play, which means that a processing entity can only ask for more information than needed for the processing activity, if such data is necessary to verify "that the person giving consent is actually the data subject".¹⁸⁵ This can especially be the case if consent is provided by telephone, or in an online environment.

Written consent of the Personal Data Law as well as the explicit consent of the GDPR have the same aim – providing the individual with better protection in situations that are considered to

¹⁸⁰ Постановление Одиннадцатого арбитражного апелляционного суда от 16 января 2017 г. N 11АП-17453/16

¹⁸¹ Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH* [2019]

¹⁸² See Chapter 4.1.1.6 Written consent

¹⁸³ See Chapter 3.1.1.6 Explicit consent

¹⁸⁴ Постановление Одиннадцатого арбитражного апелляционного суда от 16 января 2017 г. N 11АП-17453/16

¹⁸⁵ Article 29 Working Party, Opinion 15/2011 on the definition of consent [2011] WP187 (**Opinion on the Definition of Consent**) 21

be high-risk. However, while Personal Data Law chose to focus on the act of consent and define a specific form requirement, GDPR decided to focus on the criteria of unambiguity. Even though the approaches chosen are different, they can have similar results. In this way, in both jurisdictions, consent to high-risk operations cannot be implied. In fact, according to the guidance of the ICO, the consent should be “confirmed in words, rather than by any other positive action”.¹⁸⁶

GDPR’s requirement of explicit consent forces the processing entity to drive the data subject’s attention to the importance of the decision to consent, by specifically referring to the element of processing which requires specific consent.¹⁸⁷ As mentioned in Chapter 3.1.1.6, explicit consent also requires a higher standard in terms on the criteria of informed consent. In summary, by providing explicit consent, the data subject should be clear that they are consenting to a processing operation that may result in higher risk to the integrity of their personal data.

Written consent under the Personal Data Law, however, focuses on the content of the written document with which the consent should be provided. Having to sign a comprehensive document rather than providing for example, an oral consent may, in itself, warn the individual about the gravity of this action. However, considering the fact that companies in any case are required to have templates for consent to process personal data, they are likely to ask the data subject for consent in written form anyway. A data subject who is not an expert in Personal Data Law, may not recognize the difference between consent that just happens to be written and written consent in accordance with Art 9 (4) Personal Data Law. Therefore, the data subject may not recognize that the data processing they are consenting to may result in a higher risk to their personal data.

It should however be mentioned that even if GDPR does not set a form requirement, the member states are free to do so. In this way, the German Bundesdatenschutzgesetz requires the consent of employees concerning employment-related data processing to be in written form.¹⁸⁸

5.1.1.8. Duty to demonstrate consent

¹⁸⁶ Information Commissioner’s Office, ‘Consultation: GDPR consent guidance’ [2017] <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>> accessed on 11 April 2020, 18

¹⁸⁷ Luke Irvin, ‘Gaining explicit consent under the GDPR’ [2017] <<https://www.itgovernance.eu/blog/en/gaining-explicit-consent-under-the-gdpr-2>> accessed 8 May 2020

¹⁸⁸ Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 § 26 (1)

Where no reinforced consent is required, consent can be given in any form, as long as such action allows the processing party to prove that the consent was given at a later date.¹⁸⁹ In both laws, the burden of proof that consent was given lies with the processing entity.¹⁹⁰

Even though written consent is not mandatory in accordance with the GDPR, it may be sensible for traceability purposes. The Article 29 Working Party clarifies that the duty to demonstrate consent “should not in itself lead to excessive amounts of additional data processing. This means that controllers should have enough data to show a link to the processing (to show consent was obtained) but they shouldn’t be collecting any more information than necessary.”¹⁹¹ Therefore, for example, a link between consent and an IP number of the user who provided the consent should suffice, and such data as the user’s name and address should not need to be collected, unless the data needs to be processed for the specific purpose the user is consenting to. This guidance can be seen as a manifestation of the principle of data minimization.

As mentioned in Chapter 5.1.1.7 above, the information that needs to be provided with written consent in accordance with Russian Personal Data Law may force the data subject to provide more personal data to the processing entity than actually required to achieve the purpose of the processing activity.

On this occasion, it is also important to mention that companies are required to prepare templates for consent documents.¹⁹² Having to prepare and use a template may encourage companies to use generic consent documents that would cover any possible data processing activity and therefore potentially request excessive amounts of information from the data subject.

5.1.2. Withdrawal of consent

¹⁸⁹ Art 9 (1) Personal Data Law

¹⁹⁰ Art 9 (3) Personal Data Law and Art 7 (1) GDPR

¹⁹¹ Article 29 Working Party, Guidelines on consent under Regulation 2016/679 [2017] revised in 2018 (**Guidelines on Consent**) 20

¹⁹² Постановление Правительства РФ от 21.03.2012 N 211 (ред. от 06.09.2014) "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" // Первоначальный текст документа опубликован в Собр. законодательства РФ. - 02 апреля 2012 г. N 14 ст. 1626

Full control over personal data can only be assumed if the data subject not only has the right to consent, but also the right to withdraw such consent at any given time.¹⁹³ Both jurisdictions provide for such a right.

While the Personal Data Law does not set out any form requirements for a withdrawal of consent, such form requirements may and are expected to be provided by the processing entity to the data subject at the time of consent. The withdrawal template suggestion provided by Roskomnadzor¹⁹⁴ suggests that the data subject provides *inter alia* the full name and address of the controller, full name and address of the data subject and information about data subject's identification document.¹⁹⁵

According to the GDPR, withdrawing consent should be as easy as providing it. Given GDPR's principles of lawfulness, fairness and transparency, it is expected that a processing entity will have to comply with the request for withdrawal as long as it is clear that such has been placed and the consent can in fact be withdrawn in accordance with the GDPR. This makes withdrawing of consent under the GDPR easier than in accordance with the Data Protection Law, where a processing entity may disregard consent that has not been placed in accordance with the specified form requirements.

Similar to when a consent is provided, a data subject may withdraw their consent under the GDPR for a specific processing activity (granularity of consent). Such freedom of choice for a data subject is not ensured by the Personal Data Law, as the ability of the data subject to provide consent for some processing activities, but not for others, is also not possible as already explained in Chapter 5.1.1.2 above.

In accordance with the Personal Data Law, the processing entity should comply with the withdrawal request within a time-period of 30 days. GDPR is very similar in this regard, as it obliges the processing entity to process a withdrawal request immediately, but no later than one month from the request.

¹⁹³ Art 7 (3) GDPR and Art 9 (1) Russian

¹⁹⁴ Federal Service for the Supervision of Communications, Information Technology and Mass Communications (**Roskomnadzor**)

¹⁹⁵ Федеральная Служба По Надзору В Сфере Связи, Информационных Технологий И Массовых Коммуникаций, Управление Роскомнадзора по Сибирскому Федеральному Округу, „Образец документа на обработку персональных данных „Отзыв согласия на обработку персональных данных““ <<https://54.rkn.gov.ru/protection/docsamples/doc2/>> accessed on 12 April 2020

In both jurisdictions, the legal consequences of withdrawal take effect from the event of the data subject's successful withdrawal. This means that the processing of personal data before the withdrawal remains lawful. The processing entity has the right to keep processing personal data of the withdrawing data subject, only if such processing activity is allowed under certain provisions.¹⁹⁶ If there is no other reason justifying the processing of personal data, the processing entity must cease processing and delete or destroy the data.¹⁹⁷

There are however exceptions to this rule. For example, both jurisdictions effectively allow for further processing of personal data for archiving purposes. According to a clarification of Roskomnadzor, archiving of documents containing personal data are not governed by the Personal Data Law¹⁹⁸ and therefore processing of archived documents does not require the compliance with the requirements of consent.¹⁹⁹ In GDPR, archiving is named as an exception in Art 17 (2) lit d GDPR.

5.1.3. Time limitation

Time limitation is handled differently under GDPR and Personal Data Law.

For the purposes of GDPR, consent should not be regarded as a one-time activity. ICO's consent guidance speaks of a "dynamic idea of consent".²⁰⁰ It further elaborates that consent should be an "organic, ongoing and actively managed choice".²⁰¹ The duration of how long the consent lasts "will depend on the context, the scope of the original consent and the expectations of the data subject."²⁰²

¹⁹⁶ Art 9 (2) Personal Data Law and Art 6 GDPR; see also Решение Арбитражного суда Республики Бурятия от 09.07.2012 по делу N A10-125/2012 for practical application

¹⁹⁷ Art 17 (1) lit b GDPR; Art 9 (2) Personal Data Law

¹⁹⁸ Art 1 (2) 2 Personal Data Law

¹⁹⁹ Министерство Связи И Массовых Коммуникаций Российской Федерации, Федеральная Служба По Надзору В Сфере Связи, Информационных Технологий И Массовых Коммуникаций, „Разъяснения „Вопросы, Касающиеся Обработки Персональных Данных Работников, Соискателей На Замещение Вакантных Должностей, А Также Лиц, Находящихся В Кадровом Резерве““ // Подготовлен для системы Консультант Плюс // <http://www.consultant.ru/document/cons_doc_LAW_139574/> accessed on 10 April 2020

²⁰⁰ Information Commissioner's Office, 'Consultation: GDPR consent guidance' [2017] <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>> accessed on 11 April 2020, 6

²⁰¹ *ibid*

²⁰² Article 29 Working Party, Guidelines on consent under Regulation 2016/679 [2017] revised in 2018 (**Guidelines on Consent**) 21

This means that the data subject should be informed in case there is a change in data processing activity, or its purpose²⁰³ Similarly, when no changes occur, the data subject should also be informed about an ongoing activity, as well as being given the opportunity to withdraw their consent within a reasonable time period, without such notices proving disruptive. This should enable the data subject to make an informed choice continuously, not just at the moment of giving the consent. This obligation is particularly important when dealing with children.

It is also important to note that personal data should only continue to be processed under GDPR if it is still necessary for the purpose.²⁰⁴ Once the purpose has been achieved, the processing entity should cease processing, even if it technically still has valid consent.

Personal Data Law on the other hand provides for a certain time-period for which consent should be given. An expiration date for consent may be beneficial for the processing entities as they do not have to implement strategies to accommodate the “organic” consent, which is time consuming and requires more resources.

Since the period mostly set out under Personal Data Law is 75 years, such construct is most probably less beneficial for data subjects, as processing entities will rather rely on the generous time period than performing actual checks of the lawfulness ground.

5.1.4. Consent by representative

As the GDPR is silent on the possibility of consent by a representative, the processing entity would have to rely on the provisions of the local laws of the member states. For this reason, this aspect cannot be compared effectively.

However, there is a general possibility of consent being provided by a representative under the GDPR. For example, in case of information society services offered directly to a minor (age can vary in accordance with the Member State’s legislation), a consent can only be valid if given or authorized by the holder of parental responsibility over the child.²⁰⁵

²⁰³ Information Commissioner’s Office, ‘Consultation: GDPR consent guidance’ [2017] <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>> accessed on 11 April 2020, 35

²⁰⁴ See Chapter 3.1.1.2 on specific consent

²⁰⁵ Guidelines on Consent 23-24

5.2. Specific circumstances for consent

5.2.1. Consent provisions for children

Personal Data Law is silent on provision of consent by or for minors. Therefore general provisions of the civil law apply.²⁰⁶ For minors under 14 years of age consent should be provided by their legal representative. The situation is less clear for individuals between 14 and 18 years of age. In these cases it is advisable to obtain consent of both the minor and their legal representative.²⁰⁷ However, the consequences of not obtaining both consents are not clear.

In the EU, the processing entity would be well advised to look into provisions of each member state individually. However, even if according to the national law, a minor is able to provide consent after reaching a certain age, the consent still needs to hold up in accordance with the GDPR. Meaning the consent needs to be free, specific, informed and unambiguous.

When speaking about information society services, the GDPR has clearer provisions and explicitly states that data subjects may only consent to data processing after reaching a certain age. Before this, the consent should be provided by the legal representative of such minors. Due to the opening clause defined in Art 8 (1) GDPR, the age of consent may vary between 13 and 16 years depending on the member state.

Russian law, does not provide answers on certain important questions regarding consent provisions for children. At the same time, GDPR allows varying concepts and rules to be used across the EU. Furthermore, there is little to no case law clarifying the practical application of when consent can and should be provided by minors. For these and other reasons, the comparison of the laws in this respect exceeds the limits of this master thesis.

5.2.2. Imbalance of Power

Within the area of application of GDPR, any “element of inappropriate pressure or influence of data subject [...] which prevents a data subject from exercising their free will”²⁰⁸ leads to an

²⁰⁶ Часть первая Гражданского кодекса Российской Федерации от 30 ноября 1994 г. N 51-ФЗ; принят Гос. Думой Федер. Собр. Рос. Федерации 21 октября 1994 г. // Собр. законодательства РФ. – 1994. - № 32 ст. 3301 (**Russian Civil Code**) // Art 21

²⁰⁷ as discussed in more detail in Chapter 3.2.1 Consent provisions for children

²⁰⁸ Guidelines on Consent 6

invalid consent. For this reason, I would like to pay some attention to the possibilities of providing consent in the case of an imbalance of power.

As clarified in the ‘Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data published by the Council of Europe’, “[c]onsent is not freely given if there is a clear imbalance of power between the data subject and the controller, which affects the data subject’s decisions with regard to the processing.”²⁰⁹ This is the case for example the case in the field of law enforcement. Article 29 Working Party has clarified that “consent could never work as the legal basis” in such scenario.²¹⁰ The situation of imbalance of power often arises in the case of data processing in the workplace, as this will be discussed in following chapters below.

The controller may, however, rely on consent despite there being an imbalance of power, if the controller can “demonstrate that this imbalance does not exist or does not affect the consent given by the data subject.”²¹¹

Neither Personal Data Law nor the Russian legal doctrine discuss the problematic of imbalance of power. On the contrary, the instrument of consent is often used in such scenarios. It is believed that one of the aims of the regulation of the instrument of consent is to reduce the information asymmetry between the data subject and the processing entity, while providing the data subject with autonomy concerning their personal data.²¹² It is assumed that a person in possession of all necessary information is able to rationally evaluate the risks and make an informed decision.²¹³

5.2.3. Data processing in a workplace

The biggest differences in the application of the instrument of consent can be found in an employment situation. While according to the GDPR, consent from an employee for processing

²⁰⁹ Council of Europe, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data [2017] T-PD (**Guidelines on Big Data**) 5

²¹⁰ Article 29 Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) [2017] WP258 12

²¹¹ Guidelines on Big Data 5

²¹² Александр Савельев, Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» [2018] Статут

²¹³ *ibid*

of their personal data by the employer is an exception, in Russian legal practice, this instrument is used heavily.²¹⁴

In fact, Roskomnadzor²¹⁵ issued a guidance on data processing in the working environment.²¹⁶ In this guidance, Roskomnadzor focusses on cases where data processing can be undertaken without consent (i.e. where other legal basis in accordance with Art 6 Personal Data Law is applicable), for other cases, the guidance emphasizes the importance of obtaining consent. At first, this guidance may not seem too different from relevant provisions of the GDPR. For example, an employer has the right to process personal data if so authorized by law. However, cases in which the employer may process personal data on the basis of a legal requirement are very specific to certain personal data and processing operations,²¹⁷ leaving many widely used processing operations out of consideration and therefore relying on employee's consent. This can be the case when providing information to the potential employer during the recruiting process.²¹⁸

In the past Roskomnadzor has criticized employers for storing a copy of an employee's passport in their personnel file,²¹⁹ as well as providing personal data of an employee to a Bank for the purposes of opening an account for salary payments²²⁰ without employee's (written) consent.

²¹⁴ Art 86 (3) Labour Code of the Russian Federation; Art 88 Labour Code of the Russian Federation; АО "Консультант Плюс", Путеводитель по госуслугам для юридических лиц. Представление уведомления об обработке персональных данных' [2020]

²¹⁵ Federal Service for the Supervision of Communications, Information Technology and Mass Communications (**Roskomnadzor**)

²¹⁶ Министерство Связи И Массовых Коммуникаций Российской Федерации, Федеральная Служба По Надзору В Сфере Связи, Информационных Технологий И Массовых Коммуникаций, 'Разъяснения „Вопросы, Касающиеся Обработки Персональных Данных Работников, Соискателей На Замещение Вакантных Должностей, А Также Лиц, Находящихся В Кадровом Резерве“' // Подготовлен для системы Консультант Плюс // <http://www.consultant.ru/document/cons_doc_LAW_139574/> accessed on 10 April 2020

²¹⁷ Art 86 (1) Labour Code of the Russian Federation

²¹⁸ БУХ.1С, 'Получение и хранение информации: соблюдение прав субъекта персональных данных' [2011]

²¹⁹ Федеральная Служба По Надзору В Сфере Связи, Информационных Технологий И Массовых Коммуникаций, Управлением Роскомнадзора по Краснодарскому краю и Республике Адыгея выявлены нарушения законодательства о персональных данных в деятельности ООО «Лор Клиника»' [2012] <<http://rkn.gov.ru/news/regions/news15435.htm>> accessed 13 April 2020; Федеральная Служба По Надзору В Сфере Связи, Информационных Технологий И Массовых Коммуникаций, 'В Краснодарском крае в деятельности ООО «Европа-СПА» выявлены нарушения федерального законодательства в области персональных данных' [2012] <<http://rkn.gov.ru/news/regions/news15643.htm>> accessed 13 April 2020

²²⁰ Федеральная Служба По Надзору В Сфере Связи, Информационных Технологий И Массовых Коммуникаций, 'В Кировской области в деятельности МБУ «Лесопаркхоз» выявлены нарушения законодательства в сфере обработки персональных данных' [2013] <<http://rkn.gov.ru/news/regions/news18252.htm>> accessed 13 April 2020

The topic of imbalance of power, or the question in how far such consent can be free, is not addressed in Roskomnadzor's guidance.

It also needs to be considered that many data processing operations required in the employment environment will require reinforced, ie written consent.²²¹ In practice, many employers prefer to get an employee's (written) consent as a catch-all instrument for the situation where some of the processing operations are not strictly required by law.²²²

Where GDPR is applicable, the practice of obtaining unnecessary consent from employees could lead to high fines. This has recently been confirmed by the Greek Data Protection Authority in their decision No. 26/2019, in which the professional services firm PricewaterhouseCoopers was fined EUR 150,000 for asking their employees to consent to data processing operations, where in fact the processing had been based on a different processing ground.²²³

Only in very rare cases will the processing of personal data by an employer be rightfully based on consent within the jurisdiction of the GDPR. When relying on consent, the employer also needs to take into consideration any additional provisions that member states might have put into place in accordance with Rec 155 GDPR.

5.2.3.1. Recruiting process

One of the key differences when processing personal data during recruitment is that a Russia based employer may and in many cases should rely on a data subject's consent,²²⁴ while under the GDPR, consent may in fact be seen as "misleading or inherently unfair".²²⁵ Within the area of application under GDPR, the correct processing ground can be the legitimate interest of the

²²¹ see Art 88 Labour Code

²²² Елена Беляева, „Нужно ли согласие работника на обработку его персональных данных?“ [2018] БУХГАЛТЕР 911 ОКТЯБРЬ, 2018/№ 44, <<https://i.factor.ua/journals/buh911/2018/october/issue-44/article-40102.html>> accessed 13 April 2020

²²³ Hellenic Data Protection Authority v PriceWaterhouseCoopers [2019] 26/2019

²²⁴ Министерство Связи И Массовых Коммуникаций Российской Федерации, Федеральная Служба По Надзору В Сфере Связи, Информационных Технологий И Массовых Коммуникаций, „Разъяснения „Вопросы, Касающиеся Обработки Персональных Данных Работников, Соискателей На Замещение Вакантных Должностей, А Также Лиц, Находящихся В Кадровом Резерве““ // Подготовлен для системы Консультант Плюс // <http://www.consultant.ru/document/cons_doc_LAW_139574/> accessed on 10 April 2020

²²⁵ Opinion on the Definition of Consent 13

controller²²⁶ or contractual necessity.²²⁷ However, the processing entity may only process such data which is necessary for the purposes of recruitment, only as long as necessary for the particular purpose (principle of purpose limitation) and the data subject needs to be duly informed about the processing activity (principle of transparency).

A creation of a personnel reserve is a common practice in the EU and is not prohibited under the GDPR. Thus, no consent from the data subject is required in order to keep their data for potential future job vacancies under the GDPR, as long as the data subject is correctly informed about how long their data is being kept, on which basis (mostly legitimate interest), for which purposes and what rights the data subject holds. Naturally, only data relevant to the hiring should be processed.²²⁸ In contrast to the above, Personal Data Law requires a separate consent for the addition of a candidate's information into a talent pool database, as has been clarified by Roskomnadzor.²²⁹

5.2.3.2. Background checks

As clarified in 3.2.2.2, within the GDPR area of application, background checks by current, future or potential employers will mostly be based on a local law, regulation or legitimate interest. However, one should consider that the latter might be difficult to prove. Therefore, employers are advised to keep the background checks at an absolute minimum.

Within the application of the Personal Data Law, unless such checks are mandatory by law, the employers may rely on consent.

5.2.3.3. E-mails and device monitoring

Both jurisdictions differentiate between company owned and private devices. According to Personal Data Law, in cases where employees have been issued company devices like phones or laptops and the personal use of such devices had been prohibited by the internal regulations,

²²⁶ Art 6 (1) lit f GDPR

²²⁷ Art 6 (1) lit b GDPR

²²⁸ Art 5 (4) GDPR

²²⁹ Министерство Связи И Массовых Коммуникаций Российской Федерации, Федеральная Служба По Надзору В Сфере Связи, Информационных Технологий И Массовых Коммуникаций, „Разъяснения „Вопросы, Касающиеся Обработки Персональных Данных Работников, Соискателей На Замещение Вакантных Должностей, А Также Лиц, Находящихся В Кадровом Резерве““ // Подготовлен для системы Консультант Плюс // <http://www.consultant.ru/document/cons_doc_LAW_139574/> accessed on 10 April 2020

employers may monitor the information stored on such devices if the employee had previously consented to such activity.

Under GDPR, employers may succeed in proving legitimate interest in monitoring company issued devices. Due to considerations regarding imbalance of power, it is not advisable for an employer to rely on consent in this situation. Even when an employer has ensured that the monitoring of an employee's device is lawful, the data obtained by such processing should be used with caution. Work e-mails may contain highly personal matters, as the employee may use work e-mail to contact his doctor about medical treatments. The employer's legitimate interest does not outstretch to such information.

Russian based employers may not monitor employee's private phones or personal computers, even if they are used for work purposes, as would be the case if a company has a 'bring your own device' policy. Within the application of the GPDR, such devices can be monitored only if based on explicit consent. Rarely such consent can and will be considered free.

5.2.3.4. CCTV

Installing video monitoring systems at employment premises in the EU cannot be based on consent. In Russia, however, the mere installation of CCTV and monitoring of employees is not only possible, but such activity in fact, is not sanctioned by the Personal Data Law. Protection of personal data only comes into play if the video material shall be used to identify data subjects. In this case, the processing entity requires written consent of the data subject.

5.2.4. Publicly accessible data

When speaking of publicly accessible data in this context it is necessary to define the term 'publicly accessible data'.

Personal Data Law defines publicly accessible data as data that has been made accessible by a data subject's written consent, to an unlimited number of persons, in a publicly accessible source within the meaning of Art 8 (1) Personal Data Law. No further processing ground is needed for the processing entity to use personal data that has been made public in such a way. For all other personal data that may be found on the internet or in public sources, general rules of Personal Data Law apply. For the use of this data, the processing entity will be required to obtain consent, unless the processing is based on a different processing ground.

GDPR does not have any specific rules regarding personal data found in public sources. Processing entities should be well advised to look for other lawfulness grounds for the processing of data as the modalities of contacting the correct individual and obtaining consent will be difficult in most cases.

GDPR acknowledges that sensitive data that has manifestly been made public by the data subject, can be used without the data subject's further consent. This can be the case when the data subject has for example shared information about a medical condition on a social media account. Personal Data Law does not have an equivalent provision. Unless sensitive personal data has been made public upon the data subject's written consent, the general provisions of the Personal Data Law apply.

5.2.5. Automated decision making

Automated individual decision-making is considered a high-risk data processing operation in both, Personal Data Law and the GDPR. The understanding of the term "automated decision-making" is similar. Both laws name the lack of human intervention as the defining criteria. Supporting materials issued by Article 29 Working Party provide a more detailed view on the definition of the term and pay special attention to profiling as data processing activity. A lack of such clarifications by the competent authorities in respect of Personal Data Law, may lead to different conclusions by the courts on the territory of the EU and Russian Federation, whether the same activity shall be considered automated decision making.

Under Personal Data Law, the general prohibition of automated decision-making can be waived by the data subject's written consent. Comparably, according to the GDPR a data subject may agree to such processing of his data by providing the processing entity with their explicit consent.²³⁰

In both Russian Federation and the EU, processing entities have to provide data subject with all information needed for the latter to be able to understand the impact such processing of their personal data may have.²³¹ Data subject shall have the right to challenge the decision resulting

²³⁰ Whether a written consent under the Personal Data Law and the explicit consent as provided for in the GDPR provide the same level of protection is discussed in Chapter 5.1.1.7 Reinforced consent.

²³¹ Art 16 (3) Personal Data Law; Guidelines on Automated individual decision-making and Profiling

from automated processing, including profiling.²³² GDPR provides the data subject with two additional rights, which are not named in the Personal Data Law. According to the GDPR, the data subject has the right to express their point of view regarding the automated decision or obtain human intervention.

5.2.6. Can consent be harmful?

During my research I have encountered a big difference in approach between the Personal Data Law and the GDPR in respect of the question whether obtaining consent from the data subject can be harmful. Although both laws state that a processing entity shall only rely on consent when no other processing ground is applicable,²³³ there is a big contrast in Russian and EU case law when (additional) consent has been obtained from the data subject where it had not been required.

According to the Article 29 Working Party's Guidelines on Consent, the controller shall only ask the data subject to provide consent if they are able to meet all the requirements for a valid consent.²³⁴ According to Rec 42 GDPR, consent can only be free if the data subject can make a decision. If the data subject is wrongfully under the impression that they have a choice about processing of their data, the consent provided cannot be free. Therefore, such consent is deemed invalid. Additionally, the controller should avoid any confusion as to what the processing basis is due to the principle of transparency.²³⁵

Some sources suggest there is a common practice to obtain consent as an additional processing ground.²³⁶ Such practice however is not advisable. In fact, as a consequence of such practice, the processing entity may face high fines. This has been the case in Greece where the consulting company PriceWaterhouseCoopers has been fined €150,000 by the Hellenic DPA for using inappropriate legal basis for processing of their employees' personal data.²³⁷

Russian courts on the other side are in favour of the processing entity to be obtaining additional consent from data subjects. In this respect a decision of the Pskov City Court is particularly

²³² Art 22 (3) GDPR; Art 16 (3) Personal Data Law

²³³ See Chapter 5.1.1 Notion of consent

²³⁴ Guidelines on Consent, page 3

²³⁵ European Data Protection Board, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects' [2019] 7

²³⁶ Georg Fellner and others, 'Datenschutz' [2020] WEKA Verlag, Register 3 Kapitel 2 Seite 2

²³⁷ Hellenic Data Protection Authority v PriceWaterhouseCoopers [2019] 26/2019

interesting.²³⁸ In this decision the court states that since the processing of the personal data in question is allowed in accordance with Art 10 (1) 3 Personal Data Law, the processing can occur irrespective of the fact whether the data subject had provided their consent to the processing.

²³⁸ Решение Псковского городского суда Псковской области от 30 октября 2014 г. по делу № 2-3512/2014

6. CONCLUSION

In this age of information technology, it is virtually impossible to run a business without processing personal data. Technological advancement has made processing large amounts of personal data extremely easy. At the same time, it is becoming increasingly difficult for the individual to keep control of how his data is being used and by whom. Governments rightfully see a concern regarding privacy if personal data is used unfairly. This has led many countries to issue privacy laws.

Companies operating internationally on the one side are interested in processing personal data legally, but on the other side are also keen to do so in the most economical and time saving way.

After undertaking a detailed comparison of the instrument of consent in the GDPR and in Russian Personal Data Law, I have discovered that despite similar sounding provisions, consent to data processing in the EU is treated very differently to consent within the area of application of the Personal Data Law. The big differences in the practical application make it exceedingly difficult if not impossible for a processing entity operating across both regions to design a single consent policy which would fit both laws. It would be my advice to create separate consent mechanisms to fit each of the jurisdictions. In particular, the following key points should be taken into consideration.

Despite many differences in the interpretation and use of privacy laws in European Union and Russian Federation, the laws under revision have many things in common.

Personal Data Law and GDPR agree that consent is not a general permission to process data. Any data processing activity should be linked to a specifically defined purpose. Consent should be detailed and given for each processing activity separately. Data subject can even agree to high risk processing operation by providing a reinforced consent.

When providing consent, the data subject needs to have some knowledge about the processing activity in order to be able to make an informed decision. Inter alia the data subject needs to be informed of their rights in respect of their data after the consent has been provided, in particular the right to withdraw.

Consent needs to be clearly expressed and provided in a form which enables the processing entity to prove that consent was given. Pre-ticked boxes shall not be used in either of the

jurisdictions. In fact, no consent shall be provided by inactivity. There should be a clear separation of consent provisions from general terms and conditions. Consent should be provided by a separate action then agreeing to other contractual provision.

Consent can be given by a representative but for the processing entity to be able to demonstrate consent, a power of attorney or other document confirming the legal representation should be kept by the processing entity.

The more important analyses, however, lies in examining the provisions which differ. As stated by Curran, “it is only by illustrating difference that identity is possible”.²³⁹

The instrument of consent comes from the idea of giving the data subject a choice when it comes to processing of their personal data. Consent is the weakest of the processing grounds and in theory should only be used when no other processing ground is applicable. As discussed in Chapter 5.2.3. in Russia, it is very common to use consent as a security document for the case that other processing ground may be found to be not applicable. A company operating under the GDPR would be in breach of the law and may face high fines for such practices.

During the examination it became apparent that Russian courts don’t distinguish between the separate elements of consent in the same way as it is done under the GDPR. It rather seems that the validity of consent is determined holistically, rather than step-by-step by looking at each element individually.

GDPR has stronger requirements regarding the freedom of consent, as it requires companies to demonstrate that the data subject had a genuine choice. In particular, consent shall never be a precondition to the provision of services.

GDPR’s idea of consent is that of a dynamic decision.²⁴⁰ This requires a well-managed consent policy which enables the data subject to be the master of their data. Personal Data Law sees consent as a permission given for a certain period of time. This way of managing consent is

²³⁹ Vivian Grosswald Curran, ‘Cultural Immersion, Difference and Categories in U.S. Comparative Law’ [1998] *The American Journal of Comparative Law* Vol. 46, No. 1 (Winter, 1998) 43 <<https://www.jstor.org/stable/841078?seq=1>> accessed 25 March 2020

²⁴⁰ Information Commissioner’s Office, ‘Consultation: GDPR consent guidance’ [2017] <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>> accessed on 11 April 2020, 6

certainly more beneficial for the processing entities, as it requires less administration of their part.

When processing personal data of Russian citizens, a legal entity would be well advised to follow the exact wording of the Personal Data Law in its documents and pay a special attention to the wording of consent documents. In this way the consent document should inter alia include the legal definition of processing. Legal entities are required to design and use templates for various types of consent and withdrawal of consent documents. Personal Data Law has strong form requirements for a written consent – an instrument used widely.

GDPR uses explicit consent to provide additional protection to the data subject when processing activity is considered high risk. While having templates for consent and withdrawal documents may be beneficial for the processing entity, it is not required by the law.

In order to ensure compliance in each of the jurisdictions, the processing entity would be well advised to ensure any processing activity concerning minors under 18 (in Russia) and under 13-16 (depending on the member state in the EU) and requiring consent as lawfulness ground, is secured by consent from the legal representative.

One of the main questions which has been handled differently by the laws is the question of imbalance of power between the processing entity and the data subject when providing consent. This topic has a big impact on data processing in the workplace. While under GDPR an employer will very rarely be able to effectively rely on consent, under Personal Data Law consent is used widely as a catch-all provision. Such use is even recommended by the official sources.

In sum, when processing data in the area of application of the GDPR, a processing entity will be well advised to limit use of consent as a processing ground to the absolute minimum. In fact, in some cases consent can be harmful. When operating under the Personal Data Law, however, processing entities may wish to obtain consent whenever possible in order to ensure lawful processing of data subjects' personal data.

Future court practice will bring even more clarity in the topic of consent. However, judging from the current advice and practice, a closer alignment of the privacy laws of the European Union and Russian Federation is not to be expected in the near future.

7. Bibliography

David W. Kennedy, *New Approaches to Comparative Law: Comparativism and International Governance*, 1997 UTAH L. REV. 545 (1997)

Feiler L, Forgó N, 'EU-DSGVO: EU-Datenschutz-Grundverordnung: Kurzkomentar' [2017] Verlag Österreich

Feiler L, Horn B, 'Umsetzung der DSGVO in der Praxis' [2018] Verlag Österreich

Fellner G and others, 'Datenschutz' [2020] WEKA Verlag

Glenn H.P. *Comparative Legal Families and Comparative Legal Traditions* in Reinmann M. and Zimmermann R. (eds) *The Oxford Handbook of Comparative Law* (Oxford University Press 2006)

Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С. Комментарий К Федеральному Закону От 27.07.2006 N 152-ФЗ "О Персональных Данных" [2013] Подготовлен для системы КонсультантПлюс

Кайль А.Н. и Новиков Е.А., 'Комментарий к Федеральному закону от 27 июля 2006 г. N 152-ФЗ "О персональных данных"' (постатейный) [2006] Подготовлен для системы Консультант Плюс

Приезжевая А.А., Федеральный закон «О персональных данных»: научно-практический комментарий. — М.: Редакция «Российской газеты» [2015] Вып. 11. — 176 с.

Савельев А., Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» [2018] Статут

8. Articles

Coninck, Julie De, 'The Functional Method of Comparative Law: Quo Vadis?' [2010] *The Rabel Journal of Comparative and International Private Law* Bd. 74, H. 2 (April 2010) 318

Curran, Vivian Grosswald, 'Cultural Immersion, Difference and Categories in U.S. Comparative Law' [1998] *The American Journal of Comparative Law* Volume 46 Issue 1 Winter 1998 43–92

Frankenberg G, 'Critical Comparisons: Re-thinking Comparative Law' *Harvard International Law Journal* Vol. 26

Hoecke, Mark Van, 'Methodology of Comparative Legal Research' [2015] *Law and Method*, December 2015, DOI: 10.5553/REM/.000010

Macenaite, Milda and Kosta, Eleni, 'Consent for processing children's personal data in the EU: following in US footsteps?' [2017] *Information & Communications Technology Law*, 26:2, 146-197, <<https://doi.org/10.1080/13600834.2017.1321096>>

Беляева Елена, 'Нужно ли согласие работника на обработку его персональных данных?' [2018] БУХГАЛТЕР 911 ОКТЯБРЬ, 2018/№ 44

9. Annex 1: Abstract (English)

This paper analyses and compares the instrument of consent with regards to the use of personal data on one side, as defined by the Federal law of 27 June 2006 N 152-FZ “On personal data” of the Russian Federation (Personal Data Law), and the European Union’s General Data Protection Regulation (GDPR) on the other. The aim of this thesis is to determine whether it is feasible and practically desirable for companies to develop one data protection policy on consent that can comply with both laws simultaneously, when a company is subject to the privacy laws of both jurisdictions.

To answer the question above, I compared the notion of consent in both jurisdictions by looking at the relevant elements, as well as the use of consent in specific circumstances. Examples include the consent provisions for children, data processing in the workplace, publicly available data and automated decision making. This master thesis uses elements of both the functional and law-in-context methods of comparative law. The comparison takes into account the wording of the laws, legal doctrine, case law, as well as business reality.

The comparison revealed that due to significant differences between the Russian Federation and the European Union in the understanding and practical application within the instrument of consent, it is not a desirable solution to introduce one internationally applicable consent policy for companies who are subject to both laws. Finally, the thesis summarises the key points within the instrument of consent in both jurisdictions, paying specific attention to the similarities and differences regarding the use of consent in practice.

10. Annex 2: Zusammenfassung (German summary)

In dieser Masterarbeit wird das Instrument der Einwilligung in die Verarbeitung persönlicher Daten untersucht und verglichen. Verglichen wird einerseits die Definition und die praktische Anwendung der Einwilligung im Föderalen Gesetz der Russischen Föderation vom 27. Juni 2006 Nr. 152-FZ „Über Persönliche Daten“ einerseits und in der Datenschutz-Grundverordnung der Europäischen Union andererseits. Das Ziel dieser Arbeit ist es, festzustellen, ob es für ein international tätiges Unternehmen, das beiden Gesetzen unterworfen ist, möglich ist, eine Einwilligungsstrategie auszuarbeiten und zu betreiben, die dem russischen Datenschutzgesetz sowie der DSGVO standhält und ob eine solche Lösung in der Praxis wünschenswert ist.

Um die obige Frage zu beantworten, stellte ich einen Vergleich zwischen den einzelnen Elementen der Einwilligungsdefinition der beiden Gesetze an, sowie untersuchte wie die Einwilligung in bestimmten Situationen verwendet wird. Letzteres behandelt Themen wie die Bearbeitung persönlicher Daten Minderjähriger, Einwilligung im Arbeitsverhältnis, Bearbeitung öffentlich zugänglicher Daten und automatisierte Entscheidungsfindung. Diese Masterarbeit verwendet Elemente der funktionellen Rechtsvergleichsmethode, sowie der Methode Law-in-Context. Diese vergleichende Rechtsanalyse berücksichtigt den Wortlaut des Gesetzes, die Rechtslehre, die einschlägige Rechtsprechung, sowie die unternehmerische Realität.

Der Rechtsvergleich hat erhebliche Unterschiede zwischen der Europäischen Union und der Russischen Föderation offenbart, was die Interpretation des Konzeptes der Einwilligung sowie die praktische Anwendung dieses Instrumentes angeht. Aufgrund dieser Differenzen ist es keine wünschenswerte Lösung eine international anwendbare Einwilligungsstrategie zu betreiben, um den Vorgaben beider Gesetze gerecht zu werden. Zum Abschluss werden die wichtigsten Punkte des Instrumentes der Einwilligung im Russischen Datenschutzgesetz sowie der DSGVO zusammengefasst. Besondere Aufmerksamkeit wird dabei den Unterschieden und Gemeinsamkeiten in der unternehmerischen Praxis gewidmet.