Personal Data Protection and the Role of Information Commissioner in the Covid-19 Circumstances in Slovenia

Grega Rudolf[1], Polonca Kovač[2]

Abstract
The Covid-19 pandemic and the measures taken against it have had a tremendous impact in the society. As in many other countries, rapidly changing measures taken by the Slovenian government in 2020 and 2021 have created numerous challenges impacting both the citizens and the authorities, especially Information Commissioner (IC) as a national regulatory and supervising body complaint to the General Data Protection Regulation. In this paper, the Covid-19 pandemic and measures attributed to it have affected personal data protection field is explored, primarily based on the analysis of the IC's annual reports as regards the number and results of IC's inspection supervisions over the alleged infringers of individual privacy rights before and during the Covid-19 pandemic. The study also addresses written opinions provided by the IC, particularly as regards to balancing various rights, and critical assessment of the Slovenian new draft Personal Data Protection Act submitted by the Government to the Parliament in December 2021. The main findings reveal that IC has as expected much higher burden of work during Covid-19, from prevention to sanctioning measures. Moreover, the ratio of infringements and questionable or lack of balance among conflicting rights in practice and in the national law has been significantly higher as before the pandemic. This leads to the conclusion of Covid-19 and similar crises to present a major factor of deterioration of privacy as well as the rule of law. The research results offer opportunity to, scientifically and in practice, compare legal frameworks and data with other European countries and from longitudinal perspective.

Keywords: Covid-19 pandemic, personal data protection, privacy, EU GDPR, digitalisation, Information Commissioner, Slovenia

1 Introduction

Due to the Covid-19 pandemic that has steered almost every aspect of our lives since its global outbreak in 2020, our society has had to adapt to numerous changes while also having to deal with several restrictions that were imposed to citizens worldwide. The pandemic has caused governments worldwide to take extreme measures in order to limit the spread of the virus and to protect the public health system from collapse. However, rapidly changing measures taken against the spread of the virus were prominent for impacting the balance and the enforcement of many human rights such as the right to health, right to privacy, freedom of movement and the right to data protection, as well as procedural safeguards. Namely, in spite of the general strive for simplified procedures, the authorities must, even in crises, ensure a proper balance between, say, responsiveness, on the one hand, and the legal protection of human rights, on the other. This dictates the concepts of good governance as part of good public governance and constitutional democracy (Galetta et al., 2015; Kovač, 2016; Avbelj et al., 2019).

The use of technology must thus be appropriate, lawful and within the framework of privacy and personal data protection. Personal data protection is hereby a key part of information

[1] Information Commissioner of the Republic of Slovenia, Ljubljana, Slovenia.
[2] University of Ljubljana, Faculty of Public Administration, Ljubljana, Slovenia.

privacy, specifically since in the exercise of the rights of individuals privacy and personal data protection are strongly intertwined, to the extent that they are mostly considered interlocking, especially in the EU but also globally (Kuner et al., 2020; Pirc Musar et al., 2020). But theoretical guidelines are not necessarily the same as real practice, since studies show various forms of digitalisation, be it in normal or crisis driven circumstances, might and do deteriorates the rule law at the expense of efficiency, which is occurring especially in the recent years in Slovenia, Central Eastern Europe (CEE) and world-wide (see Aristovnik et al., 2021; Horvat et al., 2021; Ranchordas, 2022).

In the EU, the personal data protection is one of the pillars of the European identity, based on the cultural values of privacy protection. Normatively, the right to personal data protection is stipulated in in the Article 16 of the Treaty on the Functioning of the EU and the Article 8 of the Charter of Fundamental Rights of the European Union (EU).[3] The latter reads that everyone has the right to the protection of personal data concerning him or her. Additionally, it sets out the main principles of data protection such as that the data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified, while the compliance with these rules shall be subject to control by an independent authority. These guidelines are reflected in the rights of individuals under the General Data Protection Regulation (GDPR),[4] valid directly in all Member States since May 2016 and in force since May 2018. The GDPR has three primary goals, (1) to strengthen individual's fundamental human rights in the digital era, and (2) to offer clarification over the rules that companies and public bodies must follow, and (3) to end the fragmentation of the national systems as well as the administrative cues arising from the fundamental human rights (Senatori, 2020, pp. 159–161; Kneuper, 2020, p. 258).

In the Republic of Slovenia, personal data protection is a constitutional guarantee under Article 38 (Avbelj et al., 2019). The first Slovenian statute regulating data protection was enacted in 1999 (37 articles), with much extended Personal Data Protection Act (PDPA-1 with 117 articles)[5] from 2004, which is still in force in early 2022. However, this Act is not fully complaint to the (new rules of) GDPR. Slovenia is therefore significantly delaying its duty to harmonise national law with the directly applicable EU regulation(s). Notably, Slovenia is by far the last Member State in this respect, albeit several versions of the new Act, so called PDPA-2 have been prepared but highly criticised and presumably not coordinated due to the Covid-19 related difficulties (Pirc Musar et al., 2020). Currently, the Government submitted to the Parliament the new draft law as of December 2021, which is still very disputable, although in many systemic dilemmas rather similar, already in 2020 adopted the Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences.

In this paper an analysis was carried out to reveal how the pandemic and the measures taken against it have impacted particularly the right to data protection in the Republic of Slovenia by taking a detailed look into the work of the Information Commissioner (IC), that serves as a regulatory and supervising body complaint to the GDPR nationally. It is explored how the

[3] EU Charter, Official Journal of the EU C 83/389, 30. 3. 2010.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the EU L 119.

[5] *ZVOP-1, Zakon o varstvu osebnih podatkov*, Official Gazette of RS, nos 86/04, 113/05, 51/07, 67/07, 94/07, 177/20. The latest amendment refers to the Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences, adopted in 2020 to harmonise Slovenian law with the so called EU Police Directive.

pandemic impacted the amount and the content of (i) IC decisions while conducting supervisions and (ii) opinions on open questions, compared to the pre-Covid period. The aim of the study is to answer to the following research question: how was the IC work affected by the Covid-19 pandemic in both scope and content?

The usual qualitative research approach attributed to legal-administrative science were employed in this study. For social sciences in general, and public administration discipline in particular, the qualitative and mixed research methods, are characteristic to gather and interpret the relevant data (Mele & Belardinelli, 2018). Such an outline offers an opportunity to address the focus of the research from an interdisciplinary point of view, which is usually taken as a necessary one albeit the topic is primarily legally determined as in our case. From methodological aspect, firstly the relevant scientific literature dealing with data protection, digitalisation and the Covid-19 measures was reviewed, especially the items about Covid-19 effects on public governance bodies, and human rights limitations of digitalisation. Concretely, normative, descriptive and dogmatic methods with methods of content analysis and synthesis were applied. Further, an empirical analysis of the IC reports was made to response to the research question of the Covid-19 impact on its work. In order to provide a valuable insight into the effects of the pandemic on the work of IC case law analysis was also used with secondary and complementary sources.

In the first part of the paper, we had analysed the need to limit human rights with personal data right in focus, continuing on with the aspect on how digitalisation has tremendously impacted the enforcement of personal data protection. We had continued on with the empirical study of the IC's annual reports and the analysis of particular case studies on specifically outstanding issues that IC had dealt with in the period of the pandemic compared with the period before. In the second part of the article, we had critically assessed the draft Slovenian Personal Data Protection Act (ZVOP-2) as of December 2021 in terms of its (lack of) compliance with the GDPR and provided reasoning whether existing regulation or regulation *de lege ferenda* might offer a better solution on combating a future event such as the pandemic where one right (right to personal data) must be limited in order to protect and to ensure other. The aim of the paper is also to analyse how effective was the limitation of the right to data protection in the wake of Covid-19 pandemic in order to ensure better protection of public health and in general, and how the digitalisation affects the personal data protection. By using various research methods, we had combined the results into discussion points in order to provide insight into the researched field that could be beneficial to both scholars and practitioners in comparable countries.

2 Personal Data in the Era of Digitalisation and Covid-19 Pandemic

The development of society and its digitalisation have had a major impact on the issue of personal data protection. In the recent years, the EU has faced several challenges posed by increased digitalisation towards personal data protection. The pressure to formulate and enact regulations governing data protection in the digital era have been high. In the recent years, the EU has been more active in personal data protection where a number of legislations have been passed. First, the EU started with enacting the GDPR in 2016, while also being ready to formulate and adopt a new e-privacy regulation, Digital Services Act, Digital Markets Act and a new Artificial Intelligence regulation focused on governing the design and use of artificial intelligence systems in the EU.

The GDPR as the main piece of legislation governing the processing of personal data, establishes the main principles regarding the processing of personal data in Article 5 of the

GDPR. The regulation therefore allows for strict data accountability principles that foster data protection in the digital age, alongside principles such as lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality (Senatori, 2020, pp. 159–161; cf. Kuner et al., 2020; Pirc Musar et al., 2020).

Other issues such as data protection by design and default have also been pushed by the advances in digital technology. For example, controllers must build such systems that would *inter alia* be designed in a way that would ensure the aforementioned principles of data protection be respected and ensured in every view of processing. Advancements in digital technologies therefore stimulated higher levels of data protecting and had pushed for formulation of more technologically-adoptive EU data protection laws. In addition to the GDPR, the EU plans to adopt a new ePrivacy regulation as a measure to strengthen personal data protection in the digital era, which would represent an important tenet of data protection with the highly changing digital communication. The new ePrivacy Regulation would pose as a comprehensive set of rules that would better protect end-user data, communication confidentiality, and device integrity, which (unlike the GDPR) does not only cover the personal data but also the metadata and confidentiality requirements with the instant messaging apps such as WhatsApp and Facebook Messenger (more Macenaite, 2019, p. 765; Mahmoodi et al., 2018, p. 1516). Therefore, advanced technologies have also pushed for the creation of stricter laws that will raise the personal data protection and security for internet end-users.

With the adverse effects of Covid-19, there has been a need for the EU governments to collect data in large volumes. Advanced digital technology tools have been therefore used to monitor and collect individual data, whereas big data acquisition in the Covid-19 era poses a great threat to data protection (see more in Newlands et al., 2020, p. 7; Gazi & Gazis, 2020, p. 75). The latter could clearly be seen during the pandemic whereas with the emergence of many digital platforms, mass collection of personal data and their processing had been carried out in order to facilitate a better response to the health crisis. One of the tools used by the EU MSs governments in the wake of the pandemic has included the purpose-built tracing tools focusing on the spatial proximity between service users and subsequently tracking their private interactions. Using two closely placed smartphones the government determined whether a close proximity of an infected person contributed to Covid-19 transmissions (van Kolfschooten & de Ruijter, 2020, p. 478). In other EU countries, proximity tracking has been used as an effective way by the government to lower Covid-19 transmission rates. Other apps such as the symptom checkers have been installed in smartphones allowing the government to collect personal data, interpret and send the data to the health ministry for immediate actions, where the quarantine real-time monitoring tools were used to determine if the citizens are complying with the given sets of quarantine restrictions (Shabani et al., 2020, p. 8).

Similarly, Russia used face recognition technology to arrest and fine more than 200 people who violated the obligation of self-isolation and quarantine. Russian regulations thus stipulated that individual had to download a mobile app that allows tracking via geolocation and register with a government-approved QR code to carry out daily activities such as walking a dog, walking to a pharmacy or walking in a park. In addition to the above, instructions were also sent through the app to individuals in self-isolation and quarantine to send so called selfies oz. images of themselves, which prove that they do not violate the ordered self-isolation or quarantine (more in Reuters, 2020; Human Rights Watch, 2020). Some authors also provide several warnings about such data processing where the digital tracking apps on patients could be repurposed to target service users for other illegitimate users such a data storage, jamming, and phishing (Spadaro, 2020, p. 317).

Digitalisation within the pandemic context has therefore placed the EU MS and other governments on a thin line between personal data protection as fundamental freedoms as well as the public safety, health, well-being, and security, despite some major benefits for the citizens and public administration in general (see, for instance, Aristovnik et al., 2020). The trade-off between data protection rights and public well-being in the application of innovative digital technologies on Covid-19 have consequently greatly contributed to an eroded public trust on existing data protection. Although the data protection frameworks have been enhanced to bolster the GDPR's requirements on individual's data privacy, the pandemic has shown the need of creating faster and more flexible legal options.

Due to pandemic's measures taken to combat the spread of the virus and ensuring the citizens right to health, the measures taken had also impacted several human rights including the right to data protection. Taking into the account the Article 52 of the EU Charter as well as the Slovenian Constitution, human rights are not always absolute and that it is the subject to limitations whether one human right collide into the other. The Article 52 stipulates that any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. It also emphasises the principle of proportionality, that ensures that any action of limiting one human right towards ensuring the other must always be made only if the limitation is necessary and it genially meets the objections of general interest or the need to protect the rights and freedom of others (more in Pirc Musar et al., 2020, pp. 28–30).

With that in mind, the European Commission provided, for instance, common standards for apps to be used by the EU MSs on the fight against Covid-19. Here, the flexible standards are meant to bolster the flexibility of the existing the GDPR provisions on data protection, where those standards ensured that the contact tracing and warning apps were compliant to data protection where data security and privacy work seamlessly everywhere in the EU (Ventrella, 2020, p. 379).

Rapid digitalisation has also increased numerous challenges regarding personal data protection that takes oversees. Digitalisation has therefore enhanced more integrated international partnerships on data protection. To control international spread of Covid-19, international state cooperation has been an involuntary need for governments. With countries such as USA, the processing of personal data on their travelling citizens to determine if they are Covid-19 infected or not have raised a series of question on international cohesiveness on data protection (more in Narula, 2020, pp. 499–510). According to Boyle & Dick (2020, pp. 695–696), such discussions on convergent international data protection laws on digital technologies have been until the pandemic inexistent. As stated by the Vice President of the European Commission, there were discussions between the USA and the EU in 2021 on the common standards that will bolster data protection and privacy for their citizens even as the respective governments focus on controlling Covid-19 through regulated international travels (European Commission, 2021). By 2021, the EU and Japan created the world's largest zone of safe data flows to share Covid-19 data between the two states. In these discussions, the focus was on how the two countries can enhance personal data protection for their citizens that was shared through innovative digital technologies such as contact tracing apps (Kliem, 2021, p. 371). Therefore, digitalisation has also fostered better international state cooperation on effective standards of data protection in the wake of Covid-19 or any other major crisis (e.g. regarding finances, mass migration, wars).

3 The Analysis of the Pandemic Impact on the Slovenian IC Work

The Information Commissionaire of the Republic of Slovenia (IC) is the independent supervisory authority under the GDPR at the national level. This body was established in 2005 by joining up previous data protection inspection within the Ministry of Justice and the Public Information Commissioner, initiated in 2003 based on the national Public Information Act (FOIA).[6] The IC is a kind of special ombudsman, *sui generis* body, and independent from the government. Its work is presented among others by the annual reports on work done on the fields of data protection and access to public information that are regularly submitted for the previous calendar year to the National Assembly by 31 May each year that contains data on the work in the previous year with assessments and recommendations, which is all published online.[7]

The IC is therefore vested in protecting two fundamental human rights; the right to the protection of personal data and the right of access to public information. In both fields, there are some common issues to be applied and significant differences in both regulative and implementation levels. The IC is a part of public administration in its broadest sense, mainly through the enforcement of its competences within administrative procedures, by the subsidiary use of General Administrative Procedure Act ensuring basic constitutional guarantees and European safeguards (Pirc Musar et al., 2020; Avbelj et al., 2019; Kovač, 2016).[8] When deciding upon individual rights and obligations of applicants, controllers or any other parties to the procedure, the IC issues individual administrative acts being subjected to judicial review in administrative dispute, that is in Slovenia in front of the special administrative court and general supreme and constitutional courts. This is the case also when the IC acts at the first instance, not just for the appellate administrative acts based on the FOIA, to ensure its independence in relation towards the executive.

Nonetheless, as regards to data protection, the IC acts as an inspection body, which means that procedures are initiated *ex officio* albeit based on application of the affected individuals, while access to public information is ensured in front of the IC only at the appellate instance if the authority holding the information requested fails to meet the applicants' requests. However, the inspection procedures are regulated by the national Inspection Act from 2002 more strictly as other administrative matters to effectively protect public interest on the field, which leads to usually stronger authorisations of the IC in the supervisory capacity as opposed to its competences in other proceedings. The current PDPA-1 does not provide any legal protection of individuals affected by the controllers as required by the GDPR (Article 77 and others, on the "appeal"), since official proceeding do in principle run against the controller without the individuals having any direct rights unless they sue the controllers for the damage done in front of the general court. Or better said: if any report or complaint is lodged for the individual data breach by the individual presumably affected, it is understood by the current Slovenian legislation that the IC initiates only inspections procedure (not appellate one), however, if there is at least plausible level of such a breach and most often not acknowledging the applicant to

[6] *ZDIJZ, Zakon o dostopu do informacij javnega značaja*, Official Gazette of RS, no 24/03 and amendments. See also the Act on Information Commissioner, *ZInfP, Zakon o Informacijskem pooblaščencu,* Official Gazette of RS, nos 113/05, 51/07.

[7] See more at the webpages https://www.ip-rs.si/, where annual reports for the data protection and right to access public information are regularly published. Hereby, all general opinions and anonymised individual IC decisions as well as judgments addressing the disputed IC decisions are available.

[8] *ZUP, Zakon o splošnem upravnem postopku*, Official Gazette of RS, no 80/99 and amendments. See also the Inspection Act, *ZIN, Zakon o inšpekcijskem nadzoru*, Official Gazette of RS, no 56/02 and amendments.

have *locus standi*. In addition, the IC provides general recommendations, assessments and opinions to prevent privacy rights to be infringed by affecting concrete individuals later on.

Based on this normative analysis combining the EU and national legislation, the research on the quantity and the content of IC opinions and decisions was carried out, particularly as regards balancing various rights related to the Covid-19 era. First, we had analysed the inspection supervisions over the alleged infringers of individual personal protection rights in 2020 and 2021 as opposed to the year 2019 before the pandemic. Second, the same approach was employed as regards to the general opinions.

For the indicators specified bellow, the percentage growth or decline was explored, in order to provide better insight into the changes with respect to the period before and after the Covid-19 epidemic, with also separating the elements into whether it was done in the public or in the private sector. The following elements were studied on the field of personal data protection:

- formal reports filed by the individuals due to alleged violations of the provisions of regulations regarding their personal protection rights;
- notifications of personal data breaches, namely notifications under Article 33 of the GDPR, which impose an obligation on personal data controllers that in the event of a breach of personal data protection, they shall immediately notify the competent supervisory authority no later than 72 hours after becoming aware of the infringement (i.e. self-reporting of the infringement);
- number of IC inspection procedures carried out on suspicion of breaches of personal data;
- complaints of individuals in connection with violations of the right to access their own personal data, which poses as a key right for the individuals to ensure transparency of the processing of their personal data;
- IC opinions on assessments of the effects of regulations as regards data protection;
- written opinions, explanations and views on personal data protection issues to individuals and legal entities that have approached the IC with questions regarding the field of personal data protection.

For the indicators addressing the individual cases, we have distinguished between the public sector controllers and the private ones (Table 1), since the former have in principle stronger power and any breaches are therefore directly affecting the rule of law.

Table 1: Analysis of the selected Slovenian IC work indicators for 2019, 2020, and 2021

	2019	2020	2021	% 2020 v. 2019	% 2021 v. 2020	%2021 v. 2019
Formal violation reports	974	1,018	1,360	+4.5	+33,6	+39,6
Infringement notices	137	120	108	-12.4	-10	-21,2
Public sector	57	63	60	+10.5	-4,8	+5,3
Private sector	80	57	48	-28.7	-15,8	-40
Inspection procedures	1,183	1,208	1,127	+2.1	-6,7	-4,7
Public sector	337	405	426	+20.2	+5,2	+26,4
Private sector	846	803	701	-5.1	-12,7	-17,1
Formal complaints on violations of the access to personal data	181	226	281	+24.9	+24,3	+55,2

	2019	2020	2021	% 2020 v. 2019	% 2021 v. 2020	%2021 v. 2019
Public sector	70	77	101*	+10	+31,2	+44,3
Private sector	111	149	180	+34.2	+20,8	+62,2
Opinions on the assessments of the regulation effects on personal data protection	73	85	85	+16,4	0	+16,4
Written opinions, explanations and views on personal data protection issues	1,261	1,331	1,471	+5,6	+10,5	+16,7

Source: IC annual reports for 2019 and 2020, supplemented with provisional data on 2021 as of April 2022

By analysing the annual reports of the IC, we can see that before the Covid-19 pandemic in the year of 2019, the IC has received 974 formal violation reports by concerning individuals claiming their personal data rights were breached. IC had also received 137 formal infringement notices based on the Article 33 of the GDPR sent by the controllers. Out of those 57 were from public (health and education institutions) and 80 from private sector (banks, telecommunication providers, insurance companies, etc.). The IC has in the year 2019 conducted 1,183 inspection procedures, out of which 337 were in the public and 846 in the private sector. Based on the report of the IC the main violations in 2019 could be attributed to the lack of transparency of the personal data processing with the lack of information given by the controllers (Article 15 of the GDPR). The IC is of the opinion that the vast majority of violations could be attributed to the lack of understanding the rules of processing set by the GDPR by the controllers in practise. In the year 2019, also breaches such as negligent or inadequate security of personal data, unlawful access to personal data files, disputed processing of personal data for the purposes of direct marketing and the implementation of video surveillance of workplaces for the purpose of employee control could also be noticed.

In 2019, the IC has also received 181 formal complaints by individuals regarding their rejection of their request to access their own personal data, to acquaint themselves with their own medical documentation and with medical documentation by other eligible persons. In that regard, 70 of those complaints were filed against controllers in the public sector (in particular ministries and their constituent bodies, courts, public health institutes and social work centres) while 111 complaints were filed against controllers in the private sector (banks, insurance companies, electronic communications operators, private associations, lawyers and private healthcare providers). In the context of the pre-consultation process, the IC has in 2019 issued 73 opinions on assessments of the effects of various regulations on the protection of personal data. The IC notes in their report that there is a lack of awareness of the importance of impact assessments as a key element in the process of drafting new regulations that provide for serious encroachments on the privacy of individuals and the introduction of modern technologies. Also, in the year 2019, IC has issued 1,261 written opinions, explanations and views on personal data protection issues, which contributed to the awareness of controllers and processors and the general public to the issues regarding data protection field. Quite a vast number of opinions written concerned the protection of personal data in connection with measures against the Covid-19 pandemic.

* Out of those 18 are based on the access request based on the Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences (Official Gazette of RS, no. 177/20)

In the year 2020, the first year of the pandemic, most of the indicators analysed had risen compared with the year prior. The IC had received 1,018 formal reports on violations of personal data rules, which is 44 more than the year prior. With that in mind, the alleged claims of violations were similar in content than in the year before the pandemic with allegations against unlawful transfer of personal data to unjustified persons, use of personal data for direct marketing purposes, unlawful video surveillance, excessive collection of personal data, use of personal data for purposes contrary to the purpose of their collection, unlawful access and inadequate security of personal data. The IC had also received 120 formal notices on personal data violations by the controllers which is 17 less than the year prior. Out of 120, 57 of those were filed by the private sector controllers and 63 from public sector bodies. The IC has conducted 1,208 inspection procedures in the same years, 405 of those in public and 803 of those in private sector. Compared to 2019, when the number of inspection cases increased by 15% compared to 2018, the increase in the number of inspection cases in 2020 has somewhat stabilised– compared to 2019, where the number increased by roughly 2%. We believe that the trend of growth could be attributed to the lack of the systematic regulatory framework of the GDPR in the national law of the Republic of Slovenia.

Further, in 2020, the IC received 226 individual complaints regarding their rejection of their request to access their own personal data, to acquaint themselves with their own medical documentation and with medical documentation by other eligible persons. Complaints concerned controllers in the public sector in 77 cases (in particular ministries and their constituent bodies, education institutions, public health institutes and social work centres) and 149 complaints against controllers in the private sector (banks, electronic communications operators, private companies, lawyers and private healthcare providers). Compared with the year before the pandemic, the IC has dealt with 45 more complaints, which is roughly 25% more. The IC notices the increase in unjustified cases of unresponsiveness and/or denial of the right of access to their own personal data by employers when employees want to get acquainted with their own personal data related to their employment relationship.

In the second year of the pandemic, in 2021, most of the analysed indicators had risen once again, with the same trend seen by comparing the year 2019 and 2020. The IC has in 2021 therefore received 1,360 formal reports on violations of personal data rules, which is 39.6% more than the year 2019, before the pandemic, which is also the highest number of received reports by the IC up to date. We can therefore see quite a rapid increase of the formal reports by the individuals and legal entities by comparing the year 2020 and 2021. The reports of the violations regarded mostly the processing of personal data of the applicants which have shown interest in vaccination against Covid-19 via the e-Government website, reports regarding invitations to vaccination against Covid-19, verification of covid green pass compliance, reports for sending letters to all citizens by the Prime Minister of the Republic of Slovenia etc. In addition to the reports relating to the implementation of measures for the prevention and control of Covid-19 infections, IC notices that other reports were submitted for quite similar reasons as in previous years. Most of them were filed for the unlawful transfer of personal data to unauthorized persons, video surveillance, use of personal data for direct marketing purposes, illegal or excessive collection of personal data, use of personal data for purposes contrary to the purpose of their collection, illegal access to databases personal data and inadequate security of personal data.

The IC has also, in 2021, received 108 infringement notices based on the Article 33 of the GDPR sent by the controllers, whereas 60 of those were from public sector entities and 48 of those from the private sector entities. The latter most often referred to the transfer of personal

data to unauthorized persons, unauthorized access to personal data due to software error or abuse by employees, loss or theft of personal data holders, attacks into the information system by extortion viruses and such. In regards to comparing the year 2021 with 2019, we see a decrease of the infringement notices by roughly 21%, with the most noticeable difference seen by comparing the private sector entities, whereas the number of announced infringement notices dropped by 40%.

We may also see a quite stabilized number of conducted inspection cases in 2021 compared by the last two years, where the figure stabilized with only a small decrease of the number of procedures by 4.7% compared with the year prior the pandemic. In 2021 the IC therefore conducted 1,127 inspection procedures, out of which 426 were in the public and 701 in the private sector. However, we can observe with concern the increase of the amount of inspection procedures conducted in the public sector, whereas the number rose quite substantially in 2021 compared with the year prior the pandemic, by roughly 26.4%. The opposite trend can be seen by analysing the private sector, whereas the number of the inspection cases dropped in 2021 by 17.1% compared with the year 2019. Similar issues as the years prior are noticed by the IC, where as in the past, violations identified in 2021 were often the result of negligent or inadequate security of personal data or the intentional illegal processing of personal data by employees of personal data controllers. This has been reflected in particular in illegal access to personal data files, controversial processing of personal data for direct marketing purposes and unjustified implementation of video surveillance in the workplace in order to control employees.

In 2021 IC had also received 281 formal complaints by individuals regarding their rejection of their request to access their own personal data, to acquaint themselves with their own medical documentation and with medical documentation by other eligible persons, which substitutes for more than 55,2% increase than the year 2019, before the pandemic. We can also see that the number of complaints by individuals regarding the rejection of their request to access their own personal data has been rising year by year, with the most prominent increase seen in the private sector (e.g. banks, insurance companies, electronic communications operators, commercial and other companies) with roughly 62,5% increase in the year 2021 compared with the year 2019. Additionally, the increase can also be seen in the public sector (especially by ministries and their constituent bodies, schools, public health institutions and social work centers) with 44,3% in 2021 compared with the year 2019. The IC also notes in its report that individuals are increasingly aware of their constitutional right to be informed about the processing of their personal data, but unfortunately the responsiveness of controllers is often inadequate and the awareness of obligations in this regard is poor. Also, IC mentions that there is a number of controllers who do not have adequate procedures in place to deal with individuals' claims for rights.

The IC in their annual report notices, that controllers want to act in accordance with the regulations but need additional help and clear instructions on how to do so, while IC emphasises that this has been particularly evident in the field of education and in work environments, which has led to excessive hardships for individuals as well as for schools, private companies and other organisations. Another increase comparing the pandemic year with the year prior can be seen by IC issuing 85 formal opinions in 2020 and 2021 on assessments of the effects of regulations to the personal data protection field, which substitutes for more than 16.4 % increase than the year 2019, before the pandemic. The analysed fact could be attributed to the turbulent situation at the time of the adoption of the various rules on the epidemic and related measures. In its annual report for 2020, the IC highlights the worrying trend of unsystematic regulation of

some serious invasions of privacy and attempts to reduce the level of data protection already achieved. IC has also in 2020 issued 1,331 written opinions, explanations and views on personal data protection issues, which is 70 more than the year prior. In 2021 IC issued 1,471 written opinions, which again is an increase of 10.5% comparing with the year 2020, with the 16.7% increase comparing the year 2021 with the year 2019, before the pandemic. Moreover, the IC has also issued numerous general opinions upon the subject based on the systematic trade-off between the basic data protection related safeguards and a need for a quick and effective response to the Covid-19 spread.[9]

For instance, regarding the introduction of the mobile contact tracking application in Slovenia, the IC believes that their warnings were mostly ignored, and thus estimated that due to inadequate communication, insistence on the mandatory use of the application and other ambiguities, confidence in such a solution has declined. Namely, as described in the previous section, various apps have been developed globally to enable proximity tracking and decreasing possibilities of Covid-19 infection (Kolfschooten & de Ruijter, 2020; Shabani et al., 2020). Therefore, the Slovenian government has, during the health crisis, developed the mobile app called *"Ostani zdrav" (Stay Healthy)*[10] with the aim of recording contacts between people who have the app installed. The purpose of the mobile app was said to make it easier for epidemiologists to keep track of contacts, especially those that they don't know have happened. With the application, users were said to be warned in a safe and anonymous way that they have been exposed to a risky contact while encouraging the individual to act responsibly. Nevertheless, the IC found serious dysfunctions and concerns that forced the government to redefine the approach.

On the other hand, the IC also mentions examples of good practice, such as the introduction of e-vignettes, where the applicant has obtained IC views in a timely manner and incorporated them into the provisions of legislation. We can therefore stipulate that asking the supervisory authority their formal opinions of pre-assessment of regulation can provide a valuable assessment of the independent authority that would further ensure adequate protection of personal data. We further emphasise the importance of personal data protection in the midst of the pandemic, which can clearly be seen in the growth of the analysed cases, where the balance of one human right could easily be subordinated against the others.

5 Discussion and Critical Perspectives on the New Personal Data Protection Act

Privacy and personal data protection are considered as a crucial part of contemporary good public governance, being a set of principles and rights developed throughout European space (Galetta et al., 2015). However, all of individual principles and rights of sustainable governance and good administration must be recognised in a balanced way. When there are questions of privacy and personal data protection discussed, in particular potentially endangered by authoritative entities, broader issues occur, affecting the bases of the rule of law. With the Covid-19 pandemic, the fundamental freedoms towards personal data protection and privacy have been exemplified now more than ever (Ienca & Vayena, 2020, pp. 463–464). Yet, research studies – as conducted by Becker et al., 2020, found out that more citizens are more complacent over the importance of data protection laws in the EU countries. For an effective recovery of

[9] See the respective opinions transparently gathered and published at the IC official webpages (2020–2022), https://www.ip-rs.si/varstvo-osebnih-podatkov/varstvo-osebnih-podatkov-v-%C4%8Dasu-epidemije-koronavirusa-covid-19.

[10] See more at the official gov.si webpages (2022), https://www.gov.si/teme/koronavirus-sars-cov-2/mobilna-aplikacija-ostanizdrav/.

the economies affected by Covid-19 pandemic, before mentioned innovative digital solutions have been introduced by the EU governments. Additionally, Becker et al. lament that the EU citizens must trust innovative digital solutions that have been enacted by the government for economic recovery to be effective.

However, the innovative digital solutions applied in the economic recovery have eroded the citizen's trust on data protection laws (Sabat et al., 2020). Contrary, digital transformation and technology progress pose new concerns to data protection, as shown through personal data processing and new digital platforms to provide for a more effective anti-Covid-19 society (Newlands et al., 2020; Gazi & Gazis, 2020). Despite its benefits, digitalisation can lead to technocracy, not improvement, if the system of values, the rules, and the relations between stakeholders are inadequate (Ranchordas, 2020; Kliem, 2021). In contrast, responsiveness, especially through digitalisation, is not only a quality of private organisations but also serves as a litmus test for the public sphere to check its accountability in relation to the public and the users since it is not in conflict with democratic values. Therefore, innovation and digitalisation are growing trends also in public administration, but need to be regulated properly to ensure legal predictability and equality (Aristovnik et al., 2020). We believe that there is a need to enhance amendments in national law to cover arising and unforeseen issues such as national pandemics that may not be specifically covered in the scope of personal data protection, such as tracking apps (cf. Ventrella, 2020; Kolfschooten & de Ruijter, 2020; Shabani et al., 2020; Spadaro, 2020; cf. the Slovenian IC opinions). Namely, digitalisation has stretched the existing laws to the extreme to ensure that government policies on the pandemic such as digital contact tracing apps do not breach the rights to personal data protection under the GDPR.

In this context, it seems of particular importance also to ensure privacy and personal data rights within administrative procedure. Administrative procedure is defined as weighing between the public interest, which is primarily protected by the holder of authority like the controllers and the IC, and the private legal interests of the parties as holders of rights and obligations towards the authority. The purpose of administrative procedural rules is therefore a balanced protection of the subordinate party in the procedure, as the public interest must prevail, although not absolutely. The argument of personal data protection as a human right being an administrative relationship is based in the fact that, on one side, there is the controller which, owing to protected constitutional values is empowered to guarantee rights in relation to data subjects, while on the other it is subject to the IC supervision. The common denominator in these relationships is the public interest, i.e. concern for a proportional collection and processing of personal data in any form, while meeting the needs for such data in accordance with the regulations. It does not matter whether such needs are public or private, yet they must be defined as such by law. At the same time, they (should) imply a minimum intervention beyond the will of the data subject. Data subjects should be able to optimally use their data, except where such is limited by law because of the public interest, which implies at least a certain period of interference with the rights under the GDPR (more in Pirc Musar et al., 2020; cf. Kuner et al., 2020). In such context, the public interest can partially overlap with private interest(s), in particular as regards the implementation of data subjects' rights, yet the resolution of a potential or acute conflict of interest is still a matter of administrative relationship and procedure. The administrative procedure thus serves several functions, from ensuring an individual's rights and participation and balancing the interests to transparency, system participation and administrative efficiency (Kovač, 2016; Galetta et al., 2015).

The empirical results presented above offer several lines of thinking to be carried out in future. It was, of course, expected that we would find the higher scope of the IC work during as opposed

to pre-Covid-19 period, mainly due to two reasons. First, the Covid-19 framework has significantly enhanced digitalisation and hence data protection related issues. Second, in any crisis of major scale as the Covid-19, the authorities tend to sacrifice certain safeguards on the altar of perceived higher efficiency. Consequently, there are more concerns raised and infringements reported. Nevertheless, the increase of the IC work in Slovenia when comparing especially the 2020 to 2019 indicators, is highly worrying in some aspects. The major issue seems to be almost 25% growth of formal complaints lodged, which is in absolute figures 181 and 226 in 2019 and 2020, respectively. Additionally, even higher number can be noticed in 2021, with figure 281, which substitutes an increase of 55,2 % in 2021 compared with 2019. In terms of the theoretically and practically more concerning infringements of public controllers, since they usually have significantly stronger powers as private ones, it is again worrying that notices submitted increased by 10% in public sector as opposed to decrease of roughly 30% in private sector, although this share could be attributed to a higher awareness of people in the Covid-19 era. In this sense, an increase of written opinions on proposed legislation from 73 in 2019 to 85 in 2020 and again 85 in 2021 (16.4% growth) is also rather a positive than negative result if the IC assessment are further on followed and infringements omitted. What is most worrisome is the fact that almost all studied elements have continued to increase in the year 2021 compared with the year prior and the year 2019. The number of formal violations reports by concerning individuals claiming their personal data rights were breached increased by 33.6% in 2021 compared with the year prior, which substitutes for an increase of almost 40% more formal reports on violations of personal data rights comparing the second year of the pandemic than the year 2019, before the pandemic. Furthermore, the number of written opinions, explanations and views on personal data protection issues given by the IC had also continued to increase comparing the timeline before and after the pandemic. Every year there seems to be more written request and opinions given by the IC to the individuals and legal entities, with 70 more written opinions given by the IC in 2020 compared with 2019 and 140 more in the year 2021. It can be presumed that this increase can also (aside from the complex social circumstances regarding Covid-19 pandemic and measures taken in order to combat its spread, which substituted in the limitations of personal data protection rights) be attributed to the fact that there still seems to be the lack of (effective) regulation in the field of personal data protection in the Republic of Slovenia, with GDPR still not being implemented into the national legislation, which results in many (complex) challenges, elaborated further on .

Since any effective public policy, such as (national) data protection, is usually prepared evidence-based, one should expect that Slovenian Ministry of Justice has taken the relevant information from IC reports and theoretical elaborations on the constitutional and the EU law related law issues (see Avbelj, 2019; Pirc Musar, 2020) into account. Namely, when the GDPR as the directly applied piece of legislation in all Member States came into force in May 2018 (after being valid already since May 2016), new national solutions have been required in the interim period to comply with the hierarchically superior EU Regulation. Many countries have opted for new Personal Data Protection Acts or have amended their previous legal framework. Some of the EU MSs have taken respective steps in due time by May 2018, while some have delayed the process but no country was as disrespectful as Slovenia. The problem was that the competent national authorities, with the Ministry of Justice at the forefront, failed to prepare a new national PDPA (PDPA-2) neither on time nor appropriate in terms of various content-wise provisions. More so – the publicly available versions of draft PDPA-2 of 2017–2021 were in some parts significantly incorrect and incomparable with foreign (for example, Croatian or German) solutions, although the EU regulation should be the same for all (more in Pirc Musar et al., 2020). Therefore, despite a proactive stance of the Information Commissioner over the period of 2016 to 2022, which, among other things, tried to support the controllers by offering

analyses and guidelines on its websites and several training courses how to interpret several inconsistences between the GDPR and still in 2022 valid and not replaced PDPA-1 from 2004, there is still a number of open dilemmas, trilemmas, and even vicious circles. For instance, the attention of the responsible Ministry of Justice was often drawn to resolve certain systemic issues, for example as the ones put forward by the Ministry of Public Administration during the process of interdepartmental coordination, arguing that procedure is not just a bureaucratic obstacle and that individual provisions of the draft PDPA-2 need to be systemically amended. Still, the latest version of the draft PDPA-2, adopted by the Government (EVA 2018-2020-0045) and submitted to the Parliament in December 2021, suffers from many basic questions, mistakes and anti-constitutional "solutions" even.

As regards to the systemic and procedural provisions, there are the following selected issue to be criticised and, hopefully, further resolved in near future to comply with the GDPR, the Slovenian Constitution and national umbrella law. The most disputable provisions proposed, albeit many comments provided upon drafts from 2017 on by other ministries, IC, scholars, NGOs (e.g. Transparency International, Info House) – are still *(sic!)* embedded in the text to be adopted by the Parliament in 2022. First, there are rather crucial differences set in relation toward the same individuals whose privacy rights are regulated based solely on the status of the data holder, being public body or private entity (e.g. bank or shop),[11] even though there is well known and confirmed consistently by case-law that legal matter is defined by functional criteria; meaning that any data base controller is accountable to guarantee basic defence rights to individuals, such as impartiality, right to be heard or reasoning, regardless of its formal status, in particular when acting as an authority based on the law; so, it is unconstitutional to allow lower standards (e.g. not being obliged to prepare an explanation of the right denied in written) for private data controllers as prescribed otherwise for state authorities as also stipulated jointly by the national Administrative Procedure Act (cf. Kovač, 2016);

Further, it is unclear what are the possible mechanisms to ensure legal protection of the individuals who might feel their rights to be infringed by the data controller in a specific case. The draft PDPA-2 defines in some events (direct) access to court while mostly it pursues that the allegedly affected individual should first seek protection in front of the infringing entity itself and/or (!?) in front of the IC. Above all, in terms of the IC competence, there is a highly problematic issue of not being clear when the appellate procedure or inspections supervision is initiated, since the IC is set simultaneously as the appellate body superior to first instance data controller, as well as supervisory first instance body. Moreover, inspection procedure is in Slovenia regulated significantly stricter as other administrative affairs, hence it is questionable, if and why shall the individual affected have different rights and IC different authorisation in an appeal as opposed to inspection procedure. In addition, the Slovenian Inspection Act and attributed case law consistently takes inspection procedures as *ex officio* ones, initiated and run only when public interest is endangered and never upon the party's request. On the other hand, the draft PDPA-2 mixes public and private interest and basic types of legal relations as well as consequent rights characteristic for the individual procedure type. For example, according to the draft Act, the affected individual who would opt for inspection supervision of the IC, would

[11] There are several consistent judgment in Slovenian case law confirming such functional understanding of controllers, e.g. judgment of the Administrative Court of the Republic of Slovenia U 17/2007, 23 January 2007. Contrary, there are some specific decision, questionable from systemic aspect, as the judgment of the Supreme Court of the Republic of Slovenia X Ips 24/2018, 13 November 2019, referring to banks as not(?) being obliged to comply their privacy rights procedures with the administrative procedure safeguards (Pirc Musar et al., 2020). This judgment also seems contrary to the other case of the same court, no X Ips 4/2020, 27 May 2020, establishing the rules of systemic procedural laws (as GAPA or Criminal Procedure Act) as superior to the PDPA or FOIA.

be automatically granted the power to initiate such supervision and hold a full *locus standi* (to be so called "applicant with special position"). This is unknown and even contrary to numerous judgments of Slovenian courts in other inspection matters (see more in Pirc Musar, 2020). However, practically the same problems are evident in the already adopted Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences from 2020 (based on the EU Police Directive), which means that said issues will probably be challenged in front of the Slovenian supreme and constitutional courts, as well as European Court of Justice, rather soon.

Finally, let us expose the issue of "administrative fines" according to the GDPR (Article 58 and others), which the Slovenian system simply does not know but Slovenian representatives did not negotiate an exemption when adopting the GDPR as, for instance, Danish and Estonian colleagues. This, however, does not mean that the direct application of the GDPR would imply the creation of a new category of measures (i.e. administrative fines), but that these and other concepts should be interpreted taking into account both the GDPR and the otherwise generally applied legal order of a particular country. An example of good practice in such regard is Croatia which, despite having a similar legal system as Slovenia, took a different course in designing its PDPA: it managed to avoid the dilemmas and inconsistencies regarding primarily administrative and (merely) supplementing administrative fines envisaged by the GDPR, while at the same time ensuring an undisputed implementation of the GDPR with the adoption of the "Act implementing the GDPR" from May 2018.

In Slovenia, the currently applicable Slovenian rules on inspection, which also apply to the IC, the administrative and the misdemeanour procedures are parallel relationships, although they are based on the same state of facts and the same controller since their purpose differs: the administrative procedure focuses on *a priori* ensuring compliance with sector-specific regulations, while the misdemeanour procedure is retroactive. Moreover, in misdemeanour procedures the law provides excluding or cross guarantees of protection of the subjects under consideration, which reflect above all in the obligation to tell the truth also against oneself as opposed to the privilege against self-incrimination. The two systemic statutes upon administrative and misdemeanour procedures also provide for different legal protection. Also, only statute can define misdemeanours and judicial competence in Slovenia, while the IC is an administrative body according to the Slovenian system, yet the draft PDPA-2 define the IC to be competent to file fines, which is, again, constitutionally disputable.[12] The above applies in particular in the light of Article 83(9) of the GDPR (General conditions for imposing administrative fines), whereby in the Member States, apart from certain exceptions, the misdemeanour procedure is conducted only in court. Taking into account the direct application of the GDPR, this problem could only be overcome if the PDPA-2 explicitly repeals Article 38 of the Inspection Act, but the draft text ignores this problem totally.

In sum, several umbrella conclusions can be made. The rights to data protection have been during the Covid-19 pandemic subordinated compared to other rights and pre-Covid-19 era,

[12] Hereby, the Slovenian Supreme Court issued that the IC is still competent for misdemeanour proceedings and has the competence to fine the infringers in the judgment IV Ips 2/2021 as of 16 March 2021, but his decision refers to the misdemeanours regulated by the valid Slovenian law (PDPA-1). As expressed by the court: "*The provisions of the GDPR not only allow states to prescribe and impose (also) other sanctions for breaches of data protection rules, but - which is very much a member, in procedural terms did not replace the procedural rules of the Misdemeanour Act (ZP-1), which apply to misdemeanour proceedings, for any breach that was defined as a misdemeanour at the time of its occurrence and a sanction was prescribed for them by law.*"

which is understandable to a certain extent but not admissible when human rights and other dimensions of the rule of law are concerned. This calls for a stronger awareness of the importance of both, substantive privacy rights and procedural guarantees protecting usually inferior individuals toward the authorities to constitute the rule of law. The amount of personal data breaches found in the IC proceedings during the pandemic has risen in several indicators more in the public sector field compared with the private controllers, which confirms the basic requirement of the rule of law concept that authorities should be bound by and abide by law. Digitalisation in general, not just Covid-19 related measures, therefore requires a constant trade-off between legal certainty and democracy standards, and flexibility.

6 Conclusion

The protection of privacy and personal data in balance with other principles, such as the rule of law, transparency and accountability, should guide in particular public institutions and also private controllers in relation to individuals, to weigh more systemically and in individual cases more of these principles. The Covid-19 pandemic brought hereby even larger amount of dilemmas, which is particularly shown through a very increased volume of cases before the Information Commissioner regarding data protection rights. To build a more sustainably system in future, any country should therefore regulate the field of data protection complaints with the EU law and values. In this respect, Slovenia will need to overcome many challenges, in both regulatory and enforcement levels, firstly by adopting an undisputable new statute, and further by all authorities and individuals to develop respect for the IC decisions and opinions. Good governance can only be the result of proportional respect for all the key tenets of modern democracies, as enshrined in the EU law and national constitutional safeguards.

References

Aristovnik, A. et al. (2021). The use of ICT by local general administrative authorities during Covid-19 for a sustainable future: Comparing five European countries. *Sustainability,* 13(21), 1–20. https://doi.org/10.3390/su132111765

Avbelj, M. (ed.). (2019). *Komentar Ustave Republike Slovenije [Commentary to the Constitution of Republic of Slovenia].* New University, European Law Faculty.

European Commission (2021). Keynote Speech by Vice-President Jourová on ‘Data Privacy post-Covid-19' at Euroactive's Virtual Conference on Data Privacy. https://ec.europa.eu/commission/presscorner/detail/en/speech_21_1123

Galetta, D.–U., Hofmann, H. C. H., Puigpelat, M. O, & Ziller, J. (2015). *The General Principles of EU Administrative Procedural Law.* European Parliament.

Gazi, T., & Gazis, A. (2020). Humanitarian aid in the age of Covid-19: A review of big data crisis analytics and the General Data Protection Regulation. *International Review of the Red Cross,* 102(913), 75–94.

Gov.si, Government of the Republic of Slovenia (2022). Official webpages: Mobilna aplikacija #OstaniZdrav. https://www.gov.si/teme/koronavirus-sars-cov-2/mobilna-aplikacija-ostanizdrav/

Horvat, M., Piatek, W., Potesil, L., & Rozsnyai, K. F. (2021). Public Administration's Adaptation to Covid-19 Pandemic-Czech, Hungarian, Polish and Slovak Experience. *Central European Public Administration Review*, *19*(1), 133–158. https://doi.org/10.17573/cepar.2021.1.06

Human Rights Watch (2020). Russia: Intrusive Tracking App Wrongly Fines Muscovites. https://www.hrw.org/news/2020/05/21/russia-intrusive-tracking-app-wrongly-fines-muscovites

Ienca, M., & Vayena, E. (2020). On the responsible use of digital data to tackle the Covid-19 pandemic. *Nature Medicine*, 26(4), 463–464.

Information Commissioner of the Republic of Slovenia (IC), official webpages at https://www.ip-rs.si/.

Kliem, F. (2021). ASEAN and the EU amidst Covid-19: overcoming the self-fulfilling prophecy of realism. *Asia Europe Journal*, 19(3), 371–389.

Kneuper, R. (2020). *Translating Data Protection into Software Requirements*. In ICISSP, pp. 257–264.

Kuner, C., Bygrave, L. A. and Docksey, C. (eds.) (2020). *The EU General Data Protection Regulation (GDPR), A Commentary*. Oxford: Oxford University Press.

van Kolfschooten, H., & de Ruijter, A. (2020). Covid-19 and privacy in the European Union: A legal perspective on contact tracing. Contemporary Security Policy, 41(3), 478–491.

Kovač, P. (2016). The requirements and limits of the codification of administrative procedures in Slovenia according to European trends. *Review of Central and East European Law,* 41 (3/4), 427–61. https://doi.org/10.1163/15730352-04103007

Macenaite, M. (2019). From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society*, 19(5), 765–779.

Mahmoodi, J., Čurdová, J., Henking, C., Kunz, M., Matić, K., Mohr, P., & Vovko, M. (2018). Internet users' valuation of enhanced data protection on social media: Which aspects of privacy are worth the most? *Frontiers in psychology*, 1516.

Mele, V., & Belardinelli, P. (2018). Mixed Methods in Public Administration Research: Selecting, Sequencing, and Connecting. *Journal of Public Administration Research and Theory, 29*(2), 334–347. https://doi.org/10.1093/jopart/muy046

Narula, R. (2020). European SMEs amidst the Covid-19 crisis: assessing impact and policy responses. *Journal of Industrial and Business Economics*, 47(3), 499–510.

Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: implications for data privacy during the Covid-19 pandemic. *Big Data & Society*, 7(2), 2053951720976680.

Pirc Musar, N. (ed.) (2020). *Komentar Splošne uredbe o varstvu podatkov [Commentary to the GDPR].* Ljubljana: Official Gazette of the Republic of Slovenia.

Ranchordas, S. (2022). Empathy in the digital administrative state. *Duke Law Journal,* 72, 1–54.

Reuters (2020). Moscow deploys facial recognition technology for coronavirus quarantine. https://www.reuters.com/article/us-china-health-moscow-technology-idUSKBN20F1RZ

Sabat, I., Neuman-Böhme, S., Varghese, N. E., Barros, P. P., Brouwer, W., van Exel, J., & Stargardt, T. (2020). United but divided: Policy responses and people's perceptions in the EU during the Covid-19 outbreak. *Health Policy*, 124(9), 909–918.

Senatori, I. (2020). The European Framework Agreement on Digitalisation: a Whiter Shade of Pale? Italian Labour Law e-Journal, 13(2), 159–175.

Shabani, M., Goffin, T., & Mertes, H. (2020). Reporting, recording, and communication of Covid-19 cases in workplace: data protection as a moving target. *Journal of Law and the Biosciences*, 7(1), lsaa008.

Spadaro, A. (2020). Covid-19: Testing the limits of human rights. *European Journal of Risk Regulation*, 11(2), 317–325.

Ventrella, E. (2020). Privacy in emergency circumstances: data protection and the Covid-19 pandemic. *ERA Forum*, 21(3) pp. 379–393. Springer.