European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 185-192
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 15

*Personal Data Protection in Practice of Remote Teaching in Polish Research Universities**

Jolanta Behr
(PhD and assistant professor at the Department of Administrative Law at the Faculty of Law, Administration and Economics of University of Wrocław)

Joanna Bigos
(PhD student at the Department of Administrative Law at the Faculty of Law, Administration and Economics of University of Wrocław)

ABSTRACT The article examines personal-data protection in the practice of Polish research universities. The detailed analysis concerns, i.a., legal provisions regulating this process and detailed activities undertaken by research universities towards its implementation. Emphasis is placed on implementation of the right to personal-data protection and access thereto in the context of the application of the public-interest clause. The work contains the results of research carried out at all Polish research universities and conclusions drawn on the basis of their analysis.

1. *Introduction*

Personal data protection is key for both individuals and society. For individuals, it safeguards their interest and ensures the provision of two rights: the right to personal-data protection, which is an autonomous right; and the right to privacy, which encompasses informational autonomy,[1] *i.e.*, one's right to decide on the type and extent of information that is published about them. This autonomy does also include control over this information when it is held by third parties.[2]

Society, on the other hand, benefits from-personal data protection as it ensures that public interest is pursued: unregulated, unlawful transfer of personal data leads to multiple threats to the social order and security and might lead to an increase in crime,[3] in extreme cases resulting in the loss of national sovereignty.[4]

The notion of "public interest"[5] is a general clause that refers to the use of extra-legal criteria that are individually processed by the institutions that enforce the law. The use thereof makes it possible for institutions to take a number of various actions towards personal-data protection. On the one hand, it

* Article submitted to double blind peer review.
[1] Autonomy viewed through substantive law.
[2] J. Behr, *Przyczyny ochrony danych osobowych*, in M. Błażewski and J. Behr (eds.), *Środki prawne ochrony danych osobowych*, Wrocław, Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, 2018, 21-23. See also: M. Tzanou, *Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right,* in *International Data Privacy Law*, vol. 3, no. 2, 2013, 88-99; L.A. Bygrave, *Data protection pursuant to the right to privacy in human rights treaties*, in *International Journal of Law and Information Technology*, vol. 6, no. 3, 1998, 247-284; S. Rodotà, *Data Protection as a Fundamental Right*, in S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne and S. Nouwt (eds.), *Reinventing Data Protection?*, Dordrecht, Springer, 2009, 77-82; G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, in *Law, Governance and Technology Series*, vol. 16, no. 2, 2014, 374-375.

[3] See more in M. Nawacki, *Kryminalizacja naruszenia ochrony danych osobowych*, in *Studia Prawnoustrojowe* vol. 52, 2021, 309-325; M. Brzozowska, *Kradzież danych osobowych*, in *Marketing w Praktyce*, no. 10, 2012, 87-89; P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu*, Warszawa, Wolters Kluwer Polska, 2019, 211; I. Lipowicz, *Konstytucyjne podstawy ochrony danych osobowych*, in P. Fajgielski (ed.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin, Wydawnictwo KUL, 2008, 49; K. Sowirka, *Przestępstwo 'kradzieży tożsamości' w polskim prawie karnym*, in *Ius Novum*, vol. 10, no. 1, 2013, 64-79.
[4] M. Tzanou, *The Fundamental Right to Data Protection. Normative Value in the Context of Counter-Terrorism Surveillance*, Oxford, Hart Publishing, 2017.
[5] For more on public interest, see: A. Mednis, *Prawo do prywatności a interes publiczny*, Warszawa, Wolters Kluwer Polska, 2006; A. Żurawik, *'Interes publiczny', 'interes społeczny' i 'interes społecznie uzasadniony'. Próba dookreślenia pojęć*, in *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, vol. 75, no. 2, 2008, 57-69; E. Komierzyńska and M. Zdyb, *Klauzula interesu publicznego w działaniach administracji publicznej*, in *Annales Universitatis Mariae Curie-Skłodowska. Sectio G. Ius*, vol. 63, no. 2, 2016, 161-176; P. Górecki, *Pojęcia interes prawny i interes publiczny na tle założeń doktryny prawa*, in *Studia Administracyjne*, no. 1, 2009, 75-89.

supports personal-data protection and the right to privacy so as to ensure the well-being of the society. On the other hand, however, it allows for situations in which an institution may get involved in the sphere of rights and freedoms of the human and the citizen, provided that the law allows for such involvement. In certain legally-regulated cases, referring to the public interest makes it possible to process personal data (including sensitive data) without the knowledge and consent of the holder of those data; moreover, it results in restricting the access to the data. Hence, on a case-to-case basis, the public-interest clause does constitute a sufficient criterion for expanding or limiting the extent of the use of one's right to personal-data protection and the right to privacy.

In this context, it becomes of paramount importance that the interest evoked by the institution that processes personal data is indeed legitimate. It should be possible to account for that interest based on objective criteria[6] and data collection should be conducted in the necessary extent, time and format. Specific cases and contexts that are claimed to be conducting actions in the public interest should not simply result from current development strategies or government's policies. In these contexts, data collection would not be serving society, but rather a small, particular and elite group.

It is in the interest of those whose data are processed and gathered that the extent of data processing is as small as possible, while the processing is carried with due diligence and in compliance with legally-required procedures. Consequently, it is also important that the data be processed only by the parties who hold the consent of their holder or by the parties who have the right to process personal data based on the law.

2. *The legal basis for processing personal data in Polish law*

Access to personal data and processing thereof requires a particular legal basis. Based on the processing party, the extent of this basis might be lesser or greater. Poland has a consolidated, baseline extent of personal-data protection, designated by state law. A large number of legal acts regulate this matter, yet there is a variance in their legal importance; they have also been issued by different entities.

The sources of law, including personal-data protection, are primarily regulated in the Constitution of the Republic of Poland of 2 April 1997[7] by the rules set off in the chapter "Sources of law".[8] These specify the sources of generally[9] and internally applicable laws. The former are applicable in the country or within the entity that created them (e.g., within a particular municipality) and may concern anyone. The latter are relevant only to the parties who are subordinate to the entity that issued them. They are therefore binding internally, within that entity, *e.g.*, within a university.

Generally applicable law, which regulates personal-data protection in the entire country is mainly based on the Constitution of Poland,[10] the Act of 10 May 2018 on Personal Data Protection[11] and Regulation 2016/679 on Protection of natural persons with regard to

[6] This can be validated and assessed by an appropriate court of law through a distinct procedure (see the decree of the Provincial Administrative Court of Kielce from 17 December 2020, case no. II SA/Ke 911/20, LEX no. 3115169). In some cases, public-administration bodies may evoke the notion of public interest without any justification, thereby denying a party the ability to carry out their rights and freedoms. In practice, access to public information was denied several times, which was substantiated by personal-data protection that was in the public interest. However, that protection was hypothetical rather than real, as the administrative body was using this notion to widen the gap in access to information between administration and citizens.

[7] Journal of Laws no. 78, item 483 with later amendments; hereinafter referred to as: "The Constitution of Poland".

[8] See art. 9, 87-94 and 234 of the Constitution of Poland.

[9] In the Republic of Poland, generally-applicable law encompasses: the Constitution of Poland; international agreements that have been ratified with the prior consent expressed in a legal act; acts and statutory instruments; ratified international agreements that have not received prior consent in a legal act (the way in which ratified international agreements are constructed with or without prior legal consent are specific to Polish law. The fact that the parliament is involved in the ratification process gives the regulations specified therein primacy over other laws); and local laws and regulations. International law includes both international agreements and the legal acts of international and supernational organisations (EU). In EU law, which is a part of Polish law, these acts encompass the primary and secondary EU acts, including the founding treaties, directives, decisions (hard law), recommendations and opinions (soft law).

[10] See the overview and discussion on the most significant legal acts on personal-data protection: J. Behr, *Źródła prawa ochrony danych osobowych,* in M. Błażewski and J. Behr (eds.), *Środki prawne ochrony danych osobowych*, 42-71.

[11] Journal of Laws from 2019, item 1781.

the processing of personal data and free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).[12]

At research universities, other regulations are present beyond these acts. They are in line with generally applicable law and further delineate the rules thereof. Their goal is to adjust generally-applicable law to the conditions and peculiarities of the particular universities and their goals.

3. *Research universities: notion and meaning*

The matters pertinent to higher education in Poland are regulated by: Art. 70, section 5 of the Constitution of Poland, which introduces the notion of autonomy of the institutions of higher education;[13] and the Act of 20 July 2018 on Polish Law on Higher Education and Science,[14] which specifies the organisation and functioning of the state's higher education system.[15] That act considers universities to be the basic organisational units that carry out public actions connected to the mission of the system of science[16] and higher education.[17]

The notion of a "research university" was introduced by Art. 365, section 2, item "e" of the Law on Higher Education and Science.[18] The document established, i.a., "Excellence initiative – research university". This initiative aims to carry out the state scientific policy and the beneficiaries thereof are referred to as research universities. In legal terms, the initiative assigns additional funding[19] by the Minister of Science and Higher Education to a public[20] or non-public[21] academic university or a federation of entities that belong to higher education and science.[22] The funds are assigned based on a competition[23] and require two legal conditions to be met. In each competition, funding[24] may be attained by 10 academic universities at most.[25] The act indicates the conditions that must be met by a university for it to be able to participate in the competition.

The first competition within the initiative was announced on 26 March 2019. Out of 20 applicants, 10 winners[26] were selected:

[12] General Data Protection Regulation, *European Parliament and Council of the European Union*, L119, 4 May 2016, 1-88; hereinafter referred to as: "The GDPR".

[13] In Polish legal academic terms this is also referred to as the rule of autonomous decentralisation or administrative autonomy; see: P. Lisowski, *Podstawowe ustalenia terminologiczno-pojęciowe dotyczące organizacji prawnej administracji publicznej w ujęciu relacyjnym (dynamicznym)*, in J. Blicharz and P. Lisowski (eds.), *Prawo administracyjne, Zagadnienia ogólne i ustrojowe*, Wrocław, Wolters Kluwer Polska, 2022, 467.

[14] Journal of Laws from 2023, item 742 with later amendments.

[15] Art. 1 of the Law on Higher Education and Science.

[15] Art. 2 of the Law on Higher Education and Science holds that the mission is to teach and conduct scientific activities at the highest level, build citizenship values and participate in social growth in terms of building an innovation-based economy.

[16] The set of entities that belong to the higher-education system and science is specified by Art. 7, section 1 of the Law on Higher Education and Science.

[18] This was postulated when the Law on Higher Education and Science was being developed. H. Izdebski*, Art. 387*, in I. Izdebski and J. M. Zieliński (eds.), *Prawo o szkolnictwie wyższym i nauce*. *Komentarz*, II ed., Wrocław, Wolters Kluwer Polska, 2021, available at https://sip.lex.pl/#/commentary/587785703/659766/izdebski-hubert-zielinski-jan-michal-prawo-o-szkolnictwie-wyzszym-i-nauce-komentarz-wyd-ii?cm=URELATIONS (accessed on: 29.10.2022).

[19] To be used for maintenance and development of the research potential of the Polish higher-education institutions. For non-public academic institutions, funding may be used exclusively for research. For public institutions, it may also be used for didactic purposes.

[20] Art. 366, section 1, item 1 of the Law on Higher Education and Science.

[21] Art. 366, section 1, item 3 of the Law on Higher Education and Science.

[22] This possibility is indicated by Art. 173, section 5, item 3 of the Law on Higher Education and Science. When an academic university belongs to a federation, it may not participate in the competition alone.

[23] The "Excellence initiative – research university" programme involves periodically-issued competitions whose aim is to elevate the international impact of the work of Polish academic institutions. The details on the competition and the number of spots, pursuant to Art. 376 of the Law on Higher Education and Science, is announced on the website (so called *Biuletyn Informacji Publicznej*, a public information bulletin) of the Minister as an announcement that specifies the subject thereof, the entities allowed to participate, participation conditions, competition enrollment process (including appeals) and detailed assessment criteria. This excludes the use of the Act of 14 June 1960, the Administrative Procedure Code (Journal of Laws from 2023, item 775).

[24] Pursuant to the existing law, an increase in funding by no less than 10% of the funding provided in the year when the competition is announced can be retained for a 6-year period (the additional funding can be extended for additional 6 years); the regulations indicate that in the first competition, the funding is issued for 7 years due to the fact that the competition participants were to create 6-year plans for increasing the quality of scientific activity and teaching. See: Art. 305, sections 3 & 4; and Art. 389, section 3 of the Law on Higher Education and Science.

[25] See the detailed conditions: Art. 387, section 2; and Art. 388, section 2 of the Law on Higher Education and Science.

[26] The remaining 10 universities that participated in the competition received additional funding that amounted to 2% of the funding they were granted in 2019 pursuant

University of Warsaw, Gdańsk University of Technology, AGH University, Warsaw University of Technology, Adam Mickiewicz University, Jagiellonian University, Medical University of Gdańsk, Silesian University of Technology, University of Wrocław and Nicolaus Copernicus University.

The research-university status is granted to the best universities in the country that meet legally designated criteria in terms of staff quality and their achievements, as well as the quality of scientific activity and the education. The status provides increased state funding and is awarded for a limited time.

4. *Personal-data protection practices at research universities during distance learning*

The analysis of personal-data protection practices by the Polish research universities during the distance-learning period is based on the data obtained from those universities based on the information that was made available to the public.[27]

It mainly concerned the internal regulations and the legal practices of personal-data protection during the SARS-CoV-2 pandemic from 20 March 2020 to 15 May 2022.

All the research universities were requested to answer the same set of questions through a legally-formalised procedure based on a public-information request. There were 14 questions in total, divided into two sections. The first section contained four questions on the normative acts that regulated personal-data protection during the SARS-CoV-2 pandemic. The second section contained 10 questions and revolved around practical issues, including the number and the type of personal-data violations during that period; as well as the actions undertaken as a result in order to prevent the negative consequences of these violations. This section did also formulate questions related to the measures undertaken by the research universities so as to eliminate this kind of violations in the future.

The first section was mostly concerned with: the legal bases that regulate distance learning at particular universities (including the period, form and method); the regulations in terms of protecting private and work equipment used for distance learning; the communication channels available in distance learning; and the procedures to be followed in the case of violation of personal-data security of students and staff of research universities during distance learning. In particular, this component sought to discover the legal-determining factors for personal-data protection, *i.e.*, the sources of this law in terms of generally and internally-applicable law and unorganized legal sources, such as knowledge norms, good practices and habits.

The second section explored the methods of protecting the informational autonomy of students and employees during distant learning. The study examined, *i.a.*, the preparation of the research-university staff to properly follow the personal-data protection rules during distance learning, the source of data that were the basis to permit the particular students to participate in distance learning and electronic forms of confirming class attendance and verifying knowledge. Moreover, the section also inquired whether the universities conducted a threat analysis in terms of the communication tools used in distance learning. The efficiency of methods used was also examined; its goal was to establish if they provided personal-data protection, or whether certain security breaches did occur and if appropriate procedures of reporting the GDPR breaches were utilised.

Based on the responses, and given the normative acts that regulated distance learning at research universities, it was established that it was mainly generally-applicable law that was utilised, such as: the Constitution of Poland, the GDPR, the Act of 10 May 2018 on Personal Data Protection and the Act of 2 March 2020 on Special Solutions to Preventing, Counteracting and Combating COVID-19 and Other Infectious Diseases and Crisis Situations Caused by Them.[28] Moreover, legal acts that were the resolutions of the Minister of Science and Higher Education issued based on Art. 51a of the Law on Higher Education and Science were used; based on this law, under extraordinary

to Art. 380 of the Law on Higher Education and Science.

[27] Pursuant to Art. 1, section 1 of the Act of 6 September 2001 on Access to Public Information (Journal of Laws from 2022, item 902), the procedure specified therein makes it possible to file a request to public administration for information that pertains to public matters.

[28] In particular Art. 3 of the Act. Journal of Laws from 2023, item 1327 as amended.

circumstances that put the life or well-being of the members of the academic community in peril, the Minister may temporarily limit or put to halt the operations of universities within the country or its part given the level of the threat in a given area. The resolutions issued based on this law dictated that distance learning methods and techniques were to be applied to conducting courses online, regardless of whether the curriculum[29] had accounted for such possibility; this affected regular university courses, post-graduate studies and doctoral programmes and other forms of education that were conducted at universities and at other entities that were under the Minister's authority.

Outside of the generally-applicable law, to a certain extent, the issues of distance learning were also regulated by many normative acts and certain other legal acts and administrative acts issued by the university bodies and their assisting bodies, *e.g.*, through: rector's resolutions, vice-rector's resolutions, rector's announcements, university chancellor's announcements, vice-rector's announcements, announcements of rector's proxies, rector's decisions, vice-rector's decisions and rector's circulars, as well as the university senate's resolutions. All the normative acts undertaken by the university bodies and their assisting bodies were published on their respective websites under separate sections.

[29] Regulation of the Minister of Science and Higher Education of 11 March 2020 on the temporary limitation of the functioning of some institutions of higher education and science towards prevention, counteracting and combating COVID-19 (Journal of Laws, item 405), Regulation of the Minister of Science and Higher Education of 23 March 2020 on the temporary limitation of the functioning of some institutions of higher education and science towards prevention, counteracting and combating COVID-19 (Journal of Laws, item 511 as amended), Regulation of the Minister of Science and Higher Education of 21 May 2020 on the temporary limitation of the functioning of some institutions of higher education and science towards prevention, counteracting and combating COVID-19 (Journal of Laws, item 911), Regulation of the Minister of Science and Higher Education of 16 October 2020 on the temporary limitation of the functioning of some institutions of higher education and science towards prevention, counteracting and combating COVID-19 (Journal of Laws, item 1835) and Regulation of the Minister of Science and Higher Education of 25 February 2021 on the temporary limitation of the functioning of some institutions of higher education and science towards prevention, counteracting and combating COVID-19 (Journal of Laws, item 363), which was then waived on 10 August 2021.

The analysis of the research-university responses indicates that even prior to the pandemic, the universities were indeed ensuring proper security of their staff's work and private equipment that was used for distance learning. Alongside the legal regulations, good practices and guidelines were also formulated in this regard.

Only one out of the ten research universities indicated that it had an internal regulation that specified the safety policy within its computer network. The responses did also specify that a comprehensive solution was in place at the universities, i.e., the System for Information Security Management.

Beyond the legal regulations, university staff was also obligated to participate in trainings towards personal-data protection and teleinformatic security; those who processed personal information were also required to hold special personal credentials (internal certificates for data processing).

In the context of the regulations, a question inquired whether the universities permitted any available communication channel for distance learning. Some of the universities had recommendations for a particular environment and services, while some enumerated the allowed tools (in both cases those were environments and tools available for commercial use). In most of the cases, the communication between lecturers and students (outside of class) was based on internal-communication channels that are managed and secured by appropriate organizational units within the universities. When multiple communication channels were allowed, it was specified that these were only to be used under the condition that appropriate standards were in place for the identification and security of the transferred data. In this regard, secure solutions were promoted, matching the legal requirements in place.

In this section, the public universities indicated that their internal regulations specified the appropriate reactions (procedures, guidelines) to the instances of personal-data security violations during distance learning.

The second section of the request was related to the violations of the personal-data protection law, the actions undertaken to eliminate the violations and the outcomes of the potential violations related to distance learning during the SARS-CoV-2 pandemic.

The universities did not respond to the

questions in this section in a uniform fashion. It should be noted that answering the questions in a public-information request is obligatory as long as the matters of the inquiry pertain to public issues and are not in conflict with the public interest specified in the Introduction to this article. The response to the request itself is therefore legally regulated: the law specifies the required legal form of the response to the request and the allowed amount of time providing such response can take. Through an inquiry, a public administration does also establish whether responding to the request to the required extent might infringe on public interest, or whether it is without prejudice to the legally-protected data, secrets or security matters.

In most of the cases, the responses to the detailed questions were deemed to not constitute public information in the understanding of the Polish law and therefore did not need to be made available. That approach pertained to, *i.a.*: threat analysis and the notion of not conducting such analyses in terms of using new tools or systems; the approaches to personal-data security with the use of commercial tools and software, especially in the context of these data becoming available to unauthorised parties and the possibility of the data being damaged, modified or lost; information as to whether any incidents occurred or were reported at the university (incident is understood as an event in which integrity, confidentiality or availability of data might have been compromised, including the events which might carry negative consequences for the affected parties[30]), especially when staff and students were allowed to use their private inboxes to carry out actions related to the teaching process. The responses also clearly stated that information regarding IT systems, technical and organisational matters and the data on the incidents were the part of the documentation concerning personal-data protection at the university; that documentation was considered technical. It was argued that disclosing the data that constituted the university's internal documentation would compromise the security of information and loss of personal data, while publishing those data could lead to divulging information that could significantly affect, *i.a.*, the security of particular IT tools. As a result, it was deemed that the requested information that was technical at its core did not constitute public information.[31] The internal documents related to dealing with incidents were approached accordingly.[32]

In several cases, universities demanded that the petitioner (*i.e.*, the researchers conducting this study) justify the existence of the public interest that would validate the response from the research universities to the particular questions from the request for access to public information. The justification provided in the request was deemed insufficient to legitimise the existence of public interest. The authors justified the request as follows: a) the datapoints would be analysed alongside their counterparts from all other research universities towards establishing whether a systemic, coherent approach to personal-data protection existed during distance learning at these universities; b) the acquired data would make it possible to verify whether research universities, as public institutions, would be sufficiently protected against unlawful, unauthorized breaches of the integrity of their systems and data that they held; and c) the goal of the request was to ensure and improve the security of public interest. Withholding responses to many of the questions related to the important issues of personal-data protection and informational autonomy of an individual was thereby barred by the respondents.

The variety in the stances taken towards providing requested information on personal-data protection during distance learning is also apparent in the responses provided by some of the research universities. Those are very fragmented, fail to refer to the contents of the questions (in one of the cases, a response to all the questions consisted of five sentences total), and some of them respond to questions without providing any relevant justification whatsoever as to why the response does not encompass the entirety of the question asked. In some instances, the respondents deemed that some data did not constitute public information in the understanding of Polish law; therefore, that data were outside the scope of public interest. These actions are in conflict with common practices and existing legal requirements.

[30] Source: https://gdpr.pl/artykuly/co-to-jest-incydent.

[31] Decree of the Supreme Administrative Court of 16 March 2021, case no. III OSK 35/21.

[32] Decree of the Provincial Administrative Court of 7 July 2021, case no. II SAB/Go 77/21.

What is more, only one of the ten research universities responded to all the questions posed in the request. The answers were comprehensive, descriptive and precise. In this particular instance, no claims were made that the requested information did not constitute public information, and neither was any further justification required.

This diverse approach to responding to the questions means that it is not possible to formulate generalised conclusions that would account for personal-data protection applied in distance learning.

More importantly, however, this highlights an important issue, posing the question whether the public-interest clause in the context of personal-data protection is actually respected by Polish research universities. The diverse approach to responding to the request, as well as the form of the responses, suggest that safeguarding the public interest means that in some cases access to vital information is being restricted; in this case, it was impossible to use an administrative procedure[33] to access the data regarding whether and how personal data were protected during the pandemic. These practices do indeed limit the informational autonomy of an individual, with the public-interest clause being interpreted *ad hoc* and in an inconsistent manner, which is indicative of the risk of the instrumental use thereof. This practice does also cast doubt on the intentions of particular research universities. It is therefore impossible to establish whether their refusal to respond is indeed caused by justifying the existence of public interest or the failure to justify it, that being limited by the need of processing a significant amount of data that were not in the possession of the university when the request was filed, which would involve investing significant means and effort towards preparing the information; or whether it is used as basis to avoid answering the specific questions which would result in negative assessment of the practices applied at the universities, especially in the context of detecting and mitigating the results of the breaches in personal-data protection. This approach does also give rise to the question whether the incorrectly interpreted public-interest clause, with that interpretation being outside of the jurisdiction of administrative inquiry, does not widen the information gap between administrative bodies and the individual; and whether this does not create a tool that, when used with ill intent, may support the institutions in pursuing their own interests irrespectively of the rights and freedoms of an individual.

5. *Conclusions*

This article shows that Polish research universities have a wide array of normative acts and other legal acts that regulate the rules of personal-data protection in distance learning. This system appears to be comprehensive and sufficient as it is regulated by both generally-applicable law provided by the state and the executive acts that are issued by the supervisory bodies of the research universities. This is further supplemented by the acts issued by the university bodies and their assisting bodies.

The aim of the regulations issued during the pandemic was to reinforce and specify the existing solutions. The obligatory staff trainings in personal-data protection and teleinformatic security[34] are also praiseworthy, with the universities incorporating a variety of informational instruments and facilitating individual inquiries by creating dedicated websites.

To reach the aim of this article, a particular approach was taken, *i.e.*, filing a request for public-information access. There were risks bound to this approach, as access to relevant information is limited by the scope of the response of a given institution to the request itself. Insufficiently-detailed responses made it difficult to comprehensively assess the practical dimension of personal-data protection during distance learning at Polish research universities. One of the key rationales given by the universities when they partly denied access to information was the protection of public interest and retaining the security of their IT systems and the safety measures thereof. These practices seem reasonable and are backed by the stance taken by the President of the Personal Data Protection Office, that Office being the central public-administration body for personal-data protection pursuant to the GDPR. It is also in line with the decisions of the Polish administrative courts.

[33] This can be subject to an administrative court-inspection.

[34] In this case, it was also specified that the training does include the students.

There are, however, reasonable doubts bound to the discrepancies in the extent of the data that were made available. Each institution had a different understanding of what public information and the public interest clause were. This led to inconsistent practices in information access and the denial thereof. In some cases, the public-information clause was found to have restricted the informational autonomy of the university. This made it impossible to verify whether and to what extent personal data were being protected, whether they may have been exposed to breaches of their integrity, confidentiality and availability, and whether these resulted in negative consequences incurred by a given institution.

Moreover, examining the practices carried out by some of the research universities might be indicative of another worrying phenomenon. Once the requests for public-information access were issued for the purposes of this study, a shift was found in the practices related to personal-data protection. For some universities, changes were made to their internally-issued regulations for personal-data protection in the area pertaining to the issued request. Certain systems and procedures were tightened up, which does deserve approval. It is, however, debatable whether the denial of information access was truly motivated by safety concerns or whether it was dictated by the deliberate intent not to disclose the errors made by particular institutions.