LEXONOMICA
Vol. 15, No. 1, pp. 53–76, June 2023

LEXONOMICA

PRIVACY AND DATA PROTECTION CONCERNS IN THE REGULATORY FRAMEWORK OF SLOVENIAN ENERGY LAW

Accepted
10. 4. 2023

Revised
18. 5. 2023

Published
29. 6. 2023

ZORAN DIMOVIĆ
University of Maribor, Faculty of Law, Maribor, Slovenia
zoran.dimovic@student.um.si

CORRESPONDING AUTHOR
zoran.dimovic@student.um.si

Abstract The implementation of smart energy systems (SES) in the Slovenian energy sector has raised significant privacy and data protection concerns. The collection and processing of personal data from energy consumers, as well as cybersecurity threats, pose risks that must be addressed. The legal framework governing privacy and data protection in the energy field in Slovenia is based on the GDPR, ZOEE, ZVPot-1, ZVOP-2 and others, which impose significant obligations on entities processing personal data. To mitigate these risks, exact terminology must be used to implement privacy, data protection and also cybersecurity measures and ensure compliance with the legal framework.

Keywords
cybersecurity,
data protection,
energy law,
green and digital transformation,
privacy protection,

https://doi.org/10.18690/lexonomica.15.1.53-76.2023

University of Maribor Press

1 Introduction

The European Union (hereinafter: EU) is founded upon shared values of human dignity, freedom, democracy, equality, the rule of law, and respect for human rights. These principles are enshrined in the Charter of Fundamental Rights of the European Union (hereinafter: Charter),[1] which reaffirms the rights arising from constitutional traditions and international obligations shared by Member States. Additionally, it takes into account the powers and tasks of the EU, as well as the European Convention for the Protection of Human Rights and Fundamental Freedoms,[2] the Social Charters[3] adopted by the EU and the Council of Europe, and the case law of the Court of Justice of the European Union (hereinafter: CJEU) and the European Court of Human Rights (Johnson and Lee, 2018: 88-95). Slovenia has included human rights in its Constitution[4] (CRS) based on the subsidiarity principle.[5]

Energy law[6] governs the production, distribution, and use of energy resources, with an increasing focus on integrating green and digital transformation processes in recent years. The former refers to the shift towards renewable energy sources, while the latter denotes the incorporation of digital technologies in the energy sector. As a developing area of law, the integration of green and digital transformation into energy law and EU treaties must align with the EU's core values and objectives, including the promotion of sustainable development, non-discrimination, and the protection of fundamental rights and freedoms. Effective integration of these two processes requires significant changes to current regulatory frameworks, including the development of new legal instruments and the modification of existing ones. Compliance with energy law and EU treaties depends on several factors, including the legal and regulatory frameworks in place, the technological and environmental changes involved, and the broader social and economic context of the

[1] EU Charter of Fundamental Rights: Charter of Fundamental Rights of the European Union, OJ 2010 C 83/389.
[2] European Convention for the Protection of Human Rights and Fundamental Freedoms, signed November 4, 1950, 213 UNTS 221.
[3] European Social Charter, opened for signature October 18, 1961, 529 UNTS 89.
[4] Constitution of the Republic of Slovenia. Uradni list Republike Slovenije [Official Gazette of the Republic of Slovenia], no. 33/1991 and subsequent amendments.
[5] Article 5 of the Treaty on European Union, OJ C 326, 26.10.2012.
[6] Energy law refers to the body of legal rules, regulations, and policies governing the production, distribution, and consumption of energy resources. It covers various sectors, including traditional fossil fuel resources, renewable energy sources, and nuclear energy. Energy law seeks to ensure the efficient and safe use of energy resources while also promoting sustainable development, environmental protection, and the protection of fundamental rights and freedoms. It also involves regulating the activities of energy companies and utilities, ensuring the security of energy supplies, and promoting competition and innovation in the energy sector.

transformation. While the integration of green and digital transformation processes can increase efficiency, reduce emissions, and promote sustainability, there are concerns regarding data protection and privacy, which will be addressed through the article.

The Republic of Slovenia is actively pursuing green and digital transformation in the energy sector. To achieve its ambitious targets, as outlined in the National Energy and Climate Plan (NECP) [7] for the period 2021-2030, Slovenia is promoting the use of renewable energy sources, energy efficiency in buildings, the use of renewable energy sources in the heating and cooling sector, and supporting the deployment of electric vehicles. It is also making progress in promoting digital transformation in the energy sector, such as the deployment of smart grids and meters, demand response mechanisms, and energy communities.

However, the green and digital transformation in Slovenia raises legal concerns in relation to energy law, data protection, and privacy. Personal data collection and processing must comply with the General Data Protection Regulation (hereinafter: GDPR) and other relevant regulations to prevent unauthorised use. The increasing use of digital technology in the energy sector has also led to concerns about cybersecurity threats, necessitating the establishment of robust cybersecurity measures. The transformation presents various legal challenges, ranging from data protection and privacy concerns to intellectual property rights and consumer protection, which require attention to ensure a smooth and sustainable transition (Villarubia, 2021: 56-57). Moreover, the green and digital transformation in Slovenia's energy sector also raises questions about the compatibility of these developments with EU law, particularly in terms of fundamental rights and environmental protection. As a member state of the EU, Slovenia is bound by the EU legal framework, including the Treaty on the Functioning of the European Union (hereinafter: TFEU) and the Treaty on European Union (hereinafter: TEU). These treaties establish the EU's values and objectives, including the promotion of sustainable development and the protection of fundamental rights and freedoms. To ensure compliance with these values and objectives, Slovenia needs to integrate green and digital transformation into its energy law and regulatory framework in a

[7] National Energy and Climate Plan of Slovenia (NECP), February 2020, accessed April 10, 2023, available at: https://www.energetika-portal.si/fileadmin/dokumenti/publikacije/nepn/dokumenti/nepn_5.0_final_feb-2020.pdf.

way that is consistent with EU law. This may require amending existing legal instruments and developing new ones to reflect the changing technological and environmental landscape (Somers, 2020: 243-262). For example, Slovenia may need to update its regulations to ensure that the deployment of smart grids and smart meters, as well as the collection and processing of energy-related data, comply with EU data protection and privacy laws. By integrating green and digital transformation into its energy law and regulatory framework in a way that is consistent with these values and objectives, Slovenia can achieve a smooth and sustainable transition to a greener and more digitalised energy system.

In this article, following the introduction and methodology sections, a comprehensive analysis will be presented to better comprehend the EU's initiatives for green and digital transformation and their implications on energy law concerning data and privacy concerns. This will include an overview of the principles themselves, as well as selected international and domestic treaties and other relevant documents. Additionally, an analysis will be conducted on the constitution, ZVOP-2,[8] ZVPot-1,[9] ZOEE,[10] EZ-1,[11] proposed e-privacy regulation,[12] some provisions in the Penal code (KZ-1)[13] concerning privacy and data protection in energy law, also taking into account the differences in terminology that may raise additional legal concerns. Finally, the aforementioned will be examined in the context of data and privacy protection and Slovenia's obligations under TEU, TFEU and other international acts. The broader implications and concerns of these findings will be discussed.

2 Methodology

A mixed-methods approach was selected for this study. The desk research was conducted by employing online and literature research techniques. Throughout this research, comprehensive data was collected by scouring available literature and online resources. The literature research comprised, among other things, statutory

[8] Zakon o varstvu osebnih podatkov, Uradni list RS, No. 163/2022.
[9] Zakon o varstvu potrošnikov, Uradni list RS, No. 130/2022.
[10] Zakon o oskrbi z električno energijo, Uradni list RS, No. 172/2021.
[11] Energetski zakon, Uradni list RS, No. 65/2020.
[12] Proposal for a Regulation of the European Parliament and of the Council concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, 2017/0003 (COD).
[13] Kazenski zakonik, Uradni list RS, No. 50/2012 and 16/2023.

laws, case law, policy documents, and pertinent academic publications (Steinberg and Trubek, 2018: 1304-1337). Within this process, various techniques such as analysis, compilation, description, abstraction, classification, legal reasoning, and synthesis were employed.

Regarding the methodology, the normative-dogmatic approach was employed as the basis for the study (Ashari and Faunce, 2018: 109-132). This involved examining the current legal regulations of fundamental human rights with a focus on the protection of personal data and privacy at both the general and sectoral levels. A top-down approach was utilised, commencing with the primary EU law, including the EU Charter, the European Convention for the Protection of Human Rights and Fundamental Freedoms, the TEU, and the TFEU. The axiological method was also employed to analyse the current legal regulations beyond the existing legal boundaries, thus employing an "out of the box" approach.

Moreover, an informal logic methodology is employed throughout the article to identify and analyse fallacies, as well as to utilise evidence to substantiate the given arguments. An adherence assessment of the appropriateness of the data and privacy protection for the energy field was also conducted, whereby the fundamental rights aspect was considered. The rule of law was regarded as a value following the TEU and TFEU's primary objective, with special emphasis on legality, proportionality, equal treatment, protection of acquired rights, and legal expectations. Furthermore, the comparative legal method approach was utilised to some extent within the framework of research development, where solutions were proposed within the existing legal framework.

3 Personal data and privacy protection in the energy field on the EU level

The EU recognises the importance of protecting personal data and privacy, particularly in the energy sector (Zapf and Wartusch, 2020: 16-22). The EU's GDPR sets out strict rules for the processing of personal data, including data collected in the energy sector and applies to any processing of personal data, whether automated or manual, in connection with the provision of energy services or the operation of energy systems (Cristofaro, 2019: 16-23). This includes data collected from smart meters, energy management systems, and other energy-related devices. The EU has

several directives and regulations that address data and privacy protection in the energy sector (Close, 2019: 406-427). These, among others, include Directive (EU) 2019/692 (Gas Directive; which sets out rules on the collection, processing, and storage of data related to the provision of natural gas, including the protection of personal data),[14] Regulation (EU) 2019/941 on the risk-preparedness in the electricity sector (Electricity Regulation III; regulation sets out rules on the protection of personal data in the context of the risk-preparedness in the electricity sector, including the requirement for organisations to take appropriate measures to protect personal data),[15] Directive (EU) 2019/944 (recast: which sets out rules for the organisation of the electricity market in the EU),[16] Regulation (EU) 2019/943 (EMR) on the internal market for electricity (which sets out rules on the protection of personal data in the context of the internal market for electricity, including the establishment of a European Data protection Board)[17] and Regulation (EU) 2018/1976 (regulation sets out rules on the free flow of non-personal data in the EU, which includes data related to the energy sector).[18]

In addition to the GDPR, several EU directives address personal data and privacy protection in the energy sector (van der Pas, 2020: 232-256). For example, the EU's Energy Efficiency Directive (EED)[19] requires member states to establish energy efficiency obligation schemes, which may involve the use of energy consumption data. The directive specifies that such data must be collected, processed and used in accordance with data protection legislation. Another important EU directive in this area is the RED II directive.[20] This directive establishes binding renewable energy targets for member states and requires the use of energy management systems and other technologies to monitor and optimise energy production and consumption. Like the EED, RED II requires that personal data be collected, processed and used

[14] Directive (EU) 2019/692 of the European Parliament and of the Council of 17 April 2019 on the reduction of the impact of certain plastic products on the environment, OJ L 120, 2019, p. 1-19.
[15] Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, OJ L 158, 2019, p. 75-105.
[16] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU, OJ L 158, 2019, p. 124-240.
[17] Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity and amending Directive 2012/27/EU, OJ L 158, 2019, p. 1-73.
[18] Regulation (EU) 2018/1976 of the European Parliament and of the Council of 11 December 2018 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, OJ L 321, 2018, p. 18-28.
[19] Directive (EU) 2018/2002 of the European Parliament and of the Council of 11 December 2018 amending Directive 2012/27/EU on energy efficiency, OJ L 315, 14.11.2012, p. 1-56.
[20] Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources, OJ L 328, 21.12.2018, p. 82-209.

in compliance with data protection regulations (Van der Pas, 2020: 232-256). One of the key implications of the GDPR for the energy sector is the need for companies to ensure that they are complying with the regulation when collecting, processing, and storing personal data.

Several EU energy directives include provisions related to personal data and privacy protection along with data protectionism (Naef, 2023: 147), and these directives must be read in conjunction with the GDPR, but law terminology is not exact. For example, the recast directive and the RED II include provisions related to the collection and processing of personal data for energy market purposes. Article 50 of the RED II requires that transmission and distribution system operators provide transparent and non-discriminatory access to data related to electricity consumption and production to authorised parties, including energy service providers, energy aggregators, and other market participants. However, this provision does not relate specifically to personal data and privacy protection. Article 55 of the recast directive requires member states to ensure that "*the data exchange, including the exchange of personal data, is conducted in a secure and non-discriminatory manner, in accordance with the GDPR*". The RED II also includes provisions related to the use of personal data, with Article 20 requiring member states to ensure that "*the exchange of data is conducted in a secure and non-discriminatory manner, in accordance with the applicable data protection rules*." Additionally, among the previously mentioned provisions, the recast EPBD directive[21] includes provisions related to the use of personal data in the context of building energy performance certificates. Article 19 requires that "*personal data processed in the context of the energy performance of buildings certification shall be protected in accordance with Union and national law*." In Gas Directive II, Article 20 specifically addresses the protection of personal data, requiring that "*processing of personal data in the context of smart metering systems shall comply with the GDPR*." Similarly, Electricity Regulation III, Article 28, sets out detailed provisions (Papadopoulos and Gkonis, 2019: 1-10) on data protection, including requirements for the establishment of a data protection officer and measures to ensure the security of personal data.

In the recast directive, Article 27 also addresses the protection of personal data and requires that Member States ensure that energy suppliers and other relevant entities protect personal data in accordance with the GDPR. In EMR, Article 25 sets out

[21] Energy Performance of Buildings Directive, 2018/844, OJ L 156, 19.6.2018, p. 75–91.

detailed provisions on data protection, including requirements for data security, confidentiality, and protection, and the establishment of data protection officers. All documents mention the need to protect personal data and specify requirements for data security, data confidentiality, and data protection but the used terminology overlaps in some provisions. The overlaps in terminology between the given and those can create legal concerns related to the consistency and interpretation of the provisions concerning personal data and privacy protection. For example, if the same term is used in different provisions with slightly different definitions (like Article 55 of the recast directive versus Article 20 of RED II), it can create confusion and uncertainty for those who are trying to comply with the regulations. This can lead to inconsistent implementation of the regulations, which could ultimately weaken the protection of personal data and privacy. Moreover, the overlapping provisions can lead to conflicting obligations for companies operating in the energy sector, which may hinder their ability to comply with all relevant regulations. For example, it may not be clear which regulation takes precedence in case of conflicting requirements. Additionally, the requirements for the appointment of a data protection officer may overlap with the requirements for conducting risk assessments, potentially creating confusion for electricity companies. Finally, there may be concerns regarding the practical implementation of the requirements for data security measures. And this is on the EU level, but when that "inexact" terminology is transported to the national level, it further raises additional legal uncertainty.

4 Protection of personal data and privacy in the energy sector at the national level

The CRS recognises the protection of privacy and personal data as a fundamental human right. Article 35 of the CRS guarantees the right to privacy and personal data protection for everyone, which is ensured by law. This provision is significant as it affirms privacy as a fundamental principle of the Slovenian legal system. Article 35 is consistent with Article 7 of the Charter, which recognises the right to respect for private and family life, home, and communications. Article 38 of the CRS states: "*Everyone has the right to be informed promptly and in detail of the data collected about him and the use to which it is being put, and to have access to that data; he also has the right to have that data corrected, and to receive compensation for any damage that may have been caused thereby.*" Furthermore, Article 38 of the CRS, which guarantees the right to personal data protection, is in line with the GDPR's articles 15 and 17 on the rights of data

subjects, including the right to access, rectify, and erase personal data and also connected with Article 11 of the Charter, which also protects the right to freedom of expression and information (Jakopin and Cesar, 2019: 162-172).

This provision guarantees individuals the right to access and control their personal data and to seek redress in case of any misuse or harm caused by its collection or processing. Additionally, the CRS stipulates that personal data can only be collected, processed, and used in accordance with the law and with respect for the individual's right to privacy. For that purpose, enacted to implement GDPR, ZVOP-2 was adopted, which is the primary legislation that governs the protection of personal data in Slovenia. ZVOP-2 provides the legal framework for the protection of personal data in Slovenia and outlines the rights and responsibilities of data controllers and processors.

ZVOP-2 also includes specific rules for the processing of sensitive personal data, such as health data and data related to criminal convictions. The law prohibits the processing of such data unless explicit consent is given by the data subject or the processing is necessary for the purposes of preventive or occupational medicine. Article 6 defines sensitive personal data as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life. Article 10 states that sensitive personal data may only be processed under certain conditions, such as with the explicit consent of the data subject or if the processing is necessary for certain purposes, such as medical treatment or employment. Finally, Article 26 provides additional safeguards for the processing of sensitive personal data, requiring that such data be processed in accordance with strict security measures and that any breaches of security be promptly reported to the relevant authorities.

4.1 Principles in energy law

The energy legal framework in Slovenia for electricity consists of several laws and regulations, including, among others, its main Energy Act (EZ-1), Renewable Energy Sources Act (ZSROVE),[22] Energy Efficiency Act (ZURE),[23] Law on Electricity Supply (ZOEE) and Environmental Protection Act (ZVO-2).[24]

[22] Zakon o spodbujanju rabe obnovljivih virov energije, Uradni list RS, No. 121/2022.
[23] Zakon o učinkoviti rabi energije, Uradni list RS, No. 158/2020.
[24] Zakon o varstvu okolja, Uradni list RS, No. 44/2022.

Legal concerns related to the energy legal framework in Slovenia include data and privacy protection, environmental protection, energy efficiency, and consumer protection. These concerns are addressed through various legal provisions, such as the GDPR, ZVOP-2, ZOEE, and ZVPot-1, which regulate the collection, use, and storage of personal and technical data, as well as the protection of privacy rights. Additionally, environmental and energy efficiency concerns are addressed through various regulations and incentives aimed at reducing emissions, promoting renewable energy, and improving energy efficiency. Consumer protection concerns are addressed through various rules on the supply and pricing of energy, as well as through the ZVPot-1, which regulates contracts and consumer rights.

The principles and objectives of energy law in Slovenia include ensuring the availability, reliability, and affordability of energy, promoting sustainable energy production and consumption, and ensuring energy security. However, there are legal concerns regarding data and privacy protection in the energy sector. One of the main legal concerns is the potential for unauthorised access to sensitive data, such as energy usage patterns and personal information, by third parties. This could lead to privacy violations and the potential for identity theft, as well as the possibility of using this information for targeted marketing or other commercial purposes. Another concern is the use of advanced technologies, such as smart grids, which could potentially collect large amounts of personal data about energy consumers. It is important to ensure that appropriate safeguards are in place to protect this data and that consumers have control over how their data is collected, used, and shared (Micheletti and Trovato, 2020: 13-15).

One of the key principles of Slovenian energy law is also the promotion of energy efficiency and renewable energy sources. This is in line with sustainable development goals (Partain: 2020, 32), which aim to reduce reliance on fossil fuels and promote the use of cleaner, more sustainable sources of energy. Additionally, Slovenian energy law also emphasises the protection of the environment and human health, which are fundamental aspects of sustainable development. Another important principle of Slovenian energy law is the integration of energy policies with other policy areas. This means that energy policies must be aligned with other areas of policy, such as environmental protection, economic development, and social welfare. This ensures that energy policies contribute to sustainable development in a holistic and integrated manner (Olawuyi, 2021). Furthermore, Slovenian energy

law also emphasises the importance of public participation and stakeholder engagement in decision-making processes related to energy. This ensures that the public has a say in decisions that affect their lives and the environment and that the principles of sustainable development are taken into account in decision-making processes. Overall, the legal issues related to the principles of Slovenian energy law in light of sustainable development objectives require a comprehensive legal framework that addresses environmental protection, public participation, energy efficiency, and compliance with EU law. To summarise, the principles of Slovenian energy law are in line with the goals of sustainable development. The emphasis on energy efficiency, renewable energy sources, environmental protection, and stakeholder engagement all contribute to the achievement of sustainable development objectives in Slovenia.

Finally, there is a concern about the potential for discrimination or unequal treatment based on energy usage patterns or other personal information. It is important to ensure that energy policies and practices do not violate anti-discrimination laws and that consumers are treated fairly and equally.

4.2 Objectives to the EZ-1 and ZOEE

ZVOP-2 and GDPR provide a comprehensive framework for the processing of personal data in Slovenia. These laws regulate the collection, storage, use, and transfer of personal data, including the rights of individuals to access, modify, and delete their personal data. These laws also establish the role and responsibilities of data controllers and processors and the requirements for data protection impact assessments, data breaches, and cross-border data transfers. These principles will be further discussed in later sections.

On the other hand, EZ-1 and other relevant sector-specific regulations establish the rules for technical data protection. These laws require that technical data related to energy production, distribution, and consumption be kept confidential and secure and that access to such data be restricted to authorised personnel only. Technical data is typically protected by industry-specific regulations, such as regulations governing the electricity market or the gas market.

Legal issues can arise with the terminology of technical data in EZ-1 if combined with the Act on Electronic Communications (ZEKom-2),[25] which also contains provisions related to the protection of technical data, particularly in relation to electronic communications networks and services. Additionally, the Information Security Act (ZInfV)[26] regulates the protection of information and communication systems, including technical data. Since all together work hand in hand, legal concerns may arise in the intersection of personal data protection and technical data protection, particularly in the energy sector. For example, energy companies may need to process personal data to provide energy services but must also ensure that technical data related to energy production and consumption is kept confidential and secure. Furthermore, there may be situations where personal data is inadvertently collected along with technical data, leading to potential privacy violations.

One legal concern about the intersection of personal data protection and technical data protection, particularly in the energy sector, is the potential for conflicts between the two types of protection. Technical data may contain personal data, which requires protection under data protection laws. However, technical data is often subject to different regulations, such as regulations for the energy sector, which may not have the same requirements for data protection. In addition, the collection and processing of technical data in the energy sector may involve complex systems and networks that make it difficult to ensure the proper protection of personal data. This can lead to issues such as data breaches or unauthorised access to personal data, which can have serious consequences for individuals' privacy and data protection rights. Furthermore, the use of new technologies, such as smart grids, raises additional legal concerns about the collection and processing of personal data, as such systems may collect and process large amounts of personal data without individuals' knowledge or consent (Braüer abd Richter, 2017: 1-17). This may lead to questions about the legality of such practices and the adequacy of existing data protection laws to address these issues.

[25] Zakon o elektronskih komunikacijah, Uradni list RS, No. 130/2022.
[26] Zakon o informacijski varnosti, Uradni list RS, No. 95/2021.

Similarly, ZOEE requires energy companies to collect and process technical data related to energy production and distribution. This includes data related to the efficiency and performance of energy systems, as well as data related to renewable energy sources. One legal concern with the intersection of personal data protection and technical data protection in the energy sector is the potential for data breaches or unauthorised access to sensitive data. Both types of data are often stored and processed on the same systems, making them vulnerable to security threats. Another legal concern is the potential for misuse of personal data, particularly with regard to marketing or other commercial activities. Energy companies may be tempted to use personal data collected from customers for these purposes, which could violate data protection regulations.

4.3 Principles of data and privacy protection in the GDPR and ZVOP-2

Legal implications regarding the potential for misuse of personal data in Slovenia can be found in several legal sources. Firstly, the GDPR applies and sets out the rules for the processing of personal data, including the legal grounds for processing, the rights of data subjects, and the obligations of data controllers and processors. The GDPR also includes provisions related to the processing of personal data for marketing purposes, requiring explicit consent from the data subject for such processing. Secondly, the ZVOP-2 implements the GDPR and provides additional rules and requirements for the processing of personal data within the country. In light of the primacy of EU law, it should be emphasised that the GDPR regulation applies directly, and its provisions also apply even if, for example, the ZVOP-2 provides for different terms. ZVOP-2 also includes provisions related to the processing of personal data for marketing purposes and provides for administrative fines and other sanctions for violations of the law. Additionally, the Slovenian Advertising Act (ZMed)[27] sets out the rules for marketing and advertising activities in the country, including the requirements for transparency, accuracy, and truthfulness in advertising. The act also includes provisions related to the protection of personal data in marketing activities.

[27] Zakon o medijih, Uradni list RS, No. 82/2021.

It should be emphasised that changes to the legislation on the protection of personal data in Slovenia (particularly the adoption of the new ZVOP-2) were necessary precisely because of the GDPR and the revised Council of Europe Convention No. 108.[28] From the perspective of the final result, it was possible to assess that the provisions in the GDPR - concerning the processing of personal data based on legitimate interests, subsequent processing of personal data for other purposes, and on authorised persons, especially with the aim of unifying the regimes of personal data protection in individual member states - may represent a certain level of reduction in the achieved level of protection of personal data. The GDPR, for example, in recital 8 states that "*Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and comprehensibility with the national legal order, incorporate elements of this Regulation into their national law.*" Then, in recital 23, it draws attention to the constitutional approaches of the Member States, which may also require broader legislative regulation of legal bases for the processing of personal data, namely: "*Where reference is made to this legal basis or to this Union law, in order to specify its contents, that reference should be understood to include a reference to national law, including as interpreted by the constitutional court of the Member State concerned.*" Furthermore, the GDPR, in the second paragraph of Article 6, provides that "*Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with point (c) or (e) of the first paragraph by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing.*"

The second part of the personal data protection reform in Slovenia has already been carried out in the Personal Data Protection Act in the Treatment of Criminal Offences (ZVOPOKD).[29] With the adoption of ZVOP-2, it can be considered that the field of personal data protection in the Republic of Slovenia is systematically regulated by three central regulations: ZVOP-2, GDPR (directly applicable provisions), and ZVOPOKD. All of them also apply to the energy field.

The division between ZVOP-2 and ZVOPOKD is as follows: ZVOPOKD is a law that deals with the processing of personal data in connection with criminal offences.

[28] Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, January 28, 1981, ETS No. 108, as amended with the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, November 8, 2001, ETS No. 181.

[29] Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj, Uradni list RS, No. 177/2020.

GDPR, which is intended for ZVOP-2 as a predominantly implementing law, applies to other processing of personal data in the private and public sectors. ZVOP-2 is also a systemic law that regulates certain issues for all systems of personal data processing unless ZVOPOKD regulates them differently or regulates them independently. Following the provisions of the GDPR, ZVOP-2 also takes into account the experience and findings regarding the use of the previous ZVOP-1 from 2004, Article 38 of the CRS on the human right to personal data protection, and the existing constitutional review of the Constitutional Court of the Republic of Slovenia on the human right to personal data protection since 1992,[30] as well as the provisions of the still valid Convention No. 108.

Legal concerns related to the potential for misuse of personal data for marketing or other commercial activities can arise in cases where data controllers or processors fail to obtain proper consent for such processing or where they use personal data in ways that are not transparent or violate the rights of data subjects. If we take a closer look, the GDPR and the ZVOP-2 share many similarities in terms of protecting individuals' personal data. However, there are some legal terminology differences between the two regulations, which can lead to some uncertainty regarding the appropriate terminology and its direct application. Firstly, GDPR is an EU-wide regulation that applies to all EU member states directly and sets out uniform requirements for data protection throughout the EU, whereas ZVOP-2 is specific to Slovenia, and some data protection provisions are specifically regulated by ZVOP-2 as stated in Article 3(1). Secondly, GDPR has broader definitions of personal data and data subjects compared to ZVOP-2. GDPR in Article 4(1) defines personal data as any information that can identify an individual directly or indirectly, while ZVOP-2 in Article 1 focuses on identifying information that relates to a natural person. GDPR also provides individuals with more rights, such as the right to data portability and the right to be forgotten, which are not explicitly granted in ZVOP-2. "*Information that can identify an individual directly or indirectly*" and "*natural person*" have different legal meanings and implications. "*Information that can identify an individual directly or indirectly*" refers to any information that can be used to identify a specific

[30] Initial Decision of the Constitutional Court, no. U-I-115/92, December 24, 1992; publication: OdlUS I, 105 and Uradni list RS, No. 3/93. Two leading decisions from the intervening period are perhaps: Decision of the Constitutional Court, no. U-I-252/00, October 8, 2003; Uradni list RS, No. 105/03 and OdlUS XII, 80 and Decision of the Constitutional Court, no. U-I-298/04, October 27, 2005; Uradni list RS, No. 100/05 and OdlUS XIV, 77; no. U-I-98/11, September 26, 2012: Uradni lsit RS, No. 79/12 and no. U-I-70/12, March 21, 2014; Uradni list RS, No. 24/14 and OdlUS XX, 23.

individual, either on its own or in combination with other information. This can include personal data such as a person's name, e-mail address, phone number, IP address, or other unique identifiers. The legal concept of "*personal data*" is used in the context of data protection laws, such as the GDPR, to regulate the collection, processing, and storage of personal data. On the other hand, "*natural person*" is a legal term that refers to a human being, as opposed to a legal entity such as a company or organisation. The term is commonly used in various legal contexts, such as contract law, tort law, and criminal law. In the context of data protection laws, the term "*natural person*" is used to distinguish between data concerning individuals and data concerning legal entities.

The ZVOP-2 regulates additional matters that are left to national legislation by the GDPR. These matters include the processing of personal data of deceased persons, the processing of personal data in activities outside the scope of EU law, and the processing of personal data by the Republic of Slovenia when acting in the fields of common security and defence policy and intelligence and security activities. Since 1990, the Republic of Slovenia has had a comprehensive approach to the protection of personal data in the systemic field, which has been governed by the Personal Data Protection Act. For those areas that are regulated in Slovenia by other laws, ZVOP-2 is also applicable, particularly with regard to systemic interventions in the confidentiality of personal data or the processing of personal data. This is primarily relevant to provisions on definitions, legal grounds for the processing of personal data, processing of personal data for other purposes, and more. In essence, ZVOP-2 is a crucial instrument that aims to respect the personality and rights of individuals, pursue the principles of lawfulness, proportionality, purpose limitation, and the provision of "*anything not expressly permitted is prohibited*." This is in line with relevant decisions of the Constitutional Court, including Decision No. U-I-25/95 of November 27, 1997, Decision No. U-I-238/99 of November 9, 2000, etc."

4.4 Consumer protection

Suppose we consider aspects of privacy and personal data protection that consumer law must be addressed. Consumer protection law (ZVPot-1) sets out the rights and obligations of consumers and businesses in commercial transactions. While the law does not specifically address data and privacy protection, it includes provisions that

aim to protect consumers from unfair business practices, such as misleading advertising or the use of unfair contract terms.

However, in the context of modern commerce, personal data and privacy protection are becoming increasingly important issues. Therefore, legal concerns may arise when businesses collect and process the personal data of consumers in a way that does not comply with data protection laws (Dulić and Maravić Čelan, 2019: 39-52). For example, businesses may be collecting more data than they need or sharing the data with third parties without obtaining the consumer's consent. Such practices may violate the consumer's right to privacy and lead to legal consequences. Furthermore, ZVPot-1 requires businesses to provide consumers with clear and transparent information about the goods or services they are offering, including their features, prices, and any terms and conditions that may apply. This includes providing clear and understandable information on how the consumer's personal data will be collected, used, and protected. Failure to do so could lead to legal concerns and potential fines or penalties. Under ZVPot-1, businesses are required to protect the personal data of consumers and must obtain consent before processing their personal data for specific purposes. Consumers also have the right to access their personal data, request corrections, and object to the processing of their data.

Consent is a fundamental aspect of data protection law, and it is generally required for the processing of personal data. However, there are situations in which consent may not be required or may be avoided. For example:

1. Contractual necessity: If the processing of personal data is necessary for the performance of a contract, consent may not be required. In the context of the EZ-1, if a data controller needs to process personal data to provide energy services to a customer, consent may not be required if the processing is necessary for the performance of the contract.
2. Legal obligation: If the processing of personal data is required by law, consent may not be necessary. For example, if a data controller is required by law to process specific personal data for regulatory compliance purposes, consent may not be required.
3. Legitimate interests: If the processing of personal data is necessary for the legitimate interests of the data controller, consent may be avoided.

However, the legitimate interests must be balanced against the interests, rights, and freedoms of the data subject.

In both ZVPot-1 and the EZ-1, there are provisions that allow for the processing of personal data without consent in certain circumstances, such as for the performance of a contract or compliance with legal obligations. However, in all cases, data controllers must ensure that they comply with all applicable data protection laws and regulations and that they take appropriate measures to protect the privacy and security of personal data.

As an additional discrepancy with personal and technical data in energy law, EZ-1 regulates the energy sector in Slovenia, including the use and protection of technical data. Energy companies are required to collect and process technical data for billing and monitoring purposes, but they must also protect the confidentiality and security of this data. Legal concerns related to data and privacy protection in the intersection of ZVPot-1 and the EZ-1 may arise in cases where energy companies collect and process personal data in addition to technical data. In these situations, energy companies must ensure compliance with both ZVPot-1 and the EZ-1n, which may require additional measures to protect the privacy of personal data.

4.5 Objectives to the Penal Code

The KZ-1 of Slovenia contains several provisions related to data and privacy protection, also legitimate for energy law breaches, including the following:

1. Unauthorised Access to Computer Systems (Article 237): This provision criminalises unauthorised access to computer systems, networks, or data, which can lead to data theft, unauthorised data processing, or data breaches.
2. Unauthorised Production and Use of Personal Data (Article 140): This provision criminalises the unauthorised collection, processing, and use of personal data, which can include the collection of sensitive personal data without proper consent, or the use of personal data for commercial purposes without consent.
3. Breach of Personal Data Protection (Article 143): This provision criminalises the failure to protect personal data, including the failure to

implement adequate technical and organisational measures to ensure data security, as well as the unauthorised disclosure of personal data.

4. Violation of Privacy (Article 139): This provision criminalises the unauthorised violation of privacy, including the use of surveillance devices or the unauthorised interception of private communications.

One of the potential intersections between the KZ-1 and the EZ-1 in relation to data and privacy protection concerns is the potential for unauthorised access (Vesel and Kresal, 2018: 183-203) or sabotage of energy systems, which could compromise the confidentiality, integrity or availability of technical or personal data (Svetlič and Krajcar, 2018: 25-37). This could result in criminal liability for the perpetrator under the KZ-1, as well as potential civil liability for damages caused to the energy company or affected individuals.

Similarly, ZOEE includes provisions related to the protection of personal data and privacy, particularly in relation to the use of smart metering systems. Article 90 of ZOEE requires energy companies to ensure the protection of personal data collected through smart metering systems and to obtain the necessary consent from customers for such data collection. However, despite these provisions, there are still legal concerns regarding the protection of personal data and privacy in the energy sector in Slovenia. For example, there may be concerns related to the sharing of personal data between energy companies and third-party service providers, as well as the use of personal data for marketing or other commercial purposes without the explicit consent of customers. Additionally, there may be concerns related to the security of smart metering systems and the potential for unauthorised access to personal data through these systems.

4.6 Objectives to the e-privacy proposal

When considering data within the energy sector, it is important to analyse the impact of forthcoming regulations on digitalisation while ensuring they are consistent with other relevant sectoral regulations. The European Commission has been preparing a Proposal for an e-Privacy Regulation as part of its DSM strategy,[31] which aims to regulate digital privacy for consumers. However, due to the rapid changes in the

[31] Zakon o medijih, Uradni list RS, No. 82/2021.

digital services industry and the influence of lobbies in politics, the update of this regulation has not yet taken place. The second version has been prepared by Croatia during its presidency of the EU (January 1 to June 1, 2020). The proposal aims to harmonise legislation across the EU, thereby strengthening the single digital market. Currently, privacy in electronic communications is regulated by a directive from 2002,[32] but a new proposal for a regulation is being considered, although its adoption has been postponed to the future.

Based on the proposal for the regulation, all actors will use data (personal and technical) under the same conditions. In addition, the proposed regulation introduces three different regimes. The strictest regime would apply to service providers based in the EU offering services to EU citizens, while separate rules would exist for service providers based in the EU offering services to third countries and for providers based outside the EU offering services to EU citizens. The proposed e-Privacy regulation differs from the GDPR regulation, which, in accordance with Article 16 of the TFEU, provides for the right to data protection for all service providers equally. The new proposal is a significant departure from the original proposal, as data on the content of communications and metadata would paint a complete picture of an individual's life and habits. It is therefore important to protect this data and for electronic communication providers to have strict regulations on how they can process and store acquired data, under what conditions they can share it with third parties, and when law enforcement agencies can access such data. Currently, there are many inconsistencies, legal uncertainties, and ambiguities in the proposed regulation, and the provisions concerning the use and transfer of this data are in conflict with the GDPR. Despite the energy sector's commitment to protecting the privacy and integrity of consumer data, the proposed regulation does not provide additional protection for consumer data and does not subvert the digitisation of the energy sector. Supplying electricity and other energy services are neither information technology services nor electronic communication services. In other words, energy services differ from web services that use cookies. Regarding smart meters for electricity, gas, and heat, as well as IoT devices, electronic communication is a supportive function and not the primary purpose or carrier of the service itself. Since data on smart metering is not classified as electronic

[32] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37-47.

communication interactive content (text, video, images, sounds), the fundamental provisions of the proposed e-Privacy regulation will not be directly applicable to the energy sector. Nevertheless, smart meters and other IoT devices are classified as "terminal equipment" due to their connection to the internet or other public electronic communication networks. Therefore, the provisions of Article 8 of the proposed regulation apply to the collection of smart meter data. This provision will not directly impact the energy sector since other provisions of the proposed e-Privacy regulation, particularly Article 6 on the permitted processing of electronic communication data, are not specified for use in the energy sector. Moreover, the provisions of Article 8 of the proposed regulation overlap with specific GDPR provisions and sector-specific rules on access to data set out in Directive 2019/944 on electricity. Interpreting Article 8 of the proposed regulation differently would create serious obstacles to the use of smart meters, reducing their potential benefits (Takahashi, 2020: 1-9).

4.7 Objectives to energy legal framework from the cybersecurity aspect

Shortly, In Slovenia, there are only a few legal acts related to both energy and cybersecurity. At the moment, there is an ongoing process of accepting the Cybersecurity Directive (NIS-2)[33] into the national legal framework, but what is important is that the directive acknowledges the energy sector as its primary field.

Legal concerns regarding personal data protection in the NIS-2 directive may arise in situations where law enforcement authorities use personal data for the purpose of preventing, detecting, or prosecuting cybercrime. The law provides for the collection, processing, and storage of personal data for these purposes, but it also imposes strict limitations on the use and disclosure of such data. Another legal concern is related to the international transfer of personal data. NIS-2 requires that any transfer of personal data outside the European Union must comply with the EU data protection rules, which may present additional legal and administrative challenges. Additionally, the law also includes provisions on the notification of data breaches, which may be a source of legal concern for organisations that suffer a cyberattack that results in unauthorised access to personal data. Finally, there may

[33] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333/80, 27.12.2022, p. 80–152

be legal concerns related to the implementation of the technical and organisational measures required by the law to ensure the security of personal data. These measures may require significant investments in technology and personnel, which may pose a challenge for some organisations.

5 Conclusions

In Slovenia, energy law is a complex legal field that is constantly evolving to adapt to the changing needs of the energy sector. One of the most pressing issues in energy law today is the protection of data and privacy. With so many overlapping laws and different phrases in law terminology, the implications for energy companies can be significant.

Firstly, it is important to understand the legal framework. The country has implemented several EU directives that aim to protect personal data and privacy. The GDPR is one such directive that has been implemented, which requires energy companies to protect personal data, including information on their employees and customers. However, there are other laws that also regulate data protection in Slovenia. For example, the ZVOP-2 sets out specific requirements for the processing of personal data in Slovenia. Additionally, the Slovenian Electronic Communications Act regulates the processing of personal data in the context of electronic communications, including data collected by energy companies.

The overlap of these laws can create confusion for energy companies, who must navigate the different legal frameworks to ensure they are compliant. Additionally, the use of different phrases in law terminology can further complicate matters. These seemingly small differences can have significant implications for energy companies, which must ensure they are using the correct terminology in their policies and procedures.

This article opens several avenues for further research. A deeper analysis of international treaties on law terminology in data and privacy protection in the energy field as a starting point can be made, especially in terms of the implications, specifics and the relationship between the terminology used in individual national legal systems and the terminology implementation of international treaties. Furthermore, a similar analysis regarding the precise intersection of different laws which address

both data and privacy and personal data protection could be made for other principles of energy law and other legal principles from international treaties in general. The critical analysis could be performed for jurisdictions other than Slovenian, similarly focusing on used terminology and overlapping laws that address the same principles in the energy field.

References

Ashari N.R., Faunce, T.A. (2018) The Use of Doctrinal Legal Research Methodology in Environmental Law Research: The Case of the Indonesian Environmental Law. *Asia Pacific Journal of Environmental Law, 21*(2), p. 109-132.

Close, R. (2019) EU Energy Law and Data Protection Law: Achieving a Synergistic Relationship? *Journal of Energy & Natural Resources Law, 37*(3), p. 406-427.

Cristofaro, L. (2019) The EU General Data Protection Regulation and the Energy Sector: Compliance Challenges and Opportunities. *International Energy Law Review, 38*(1), p. 16-23.

Dulić, I., Maravić Čelan, S. (2019) Privacy and Data Protection Issues in E-commerce. *Journal of Contemporary Economic and Business Issues, 6*(1), p. 39-52.

Jakopin, P., Cesar, U. (2019) The Protection of Personal Data in the Slovenian Legal System. *Journal of International Commercial Law and Technology, 14*(4), p. 162-172.

Johnson, L. and Lee, D. (2018) Protecting Human Rights in the Workplace. *Harvard Business Review,* p. 88-95.

Micheletti, G., Trovato, M. (2020) Data Protection in the Energy Sector: Challenges and Opportunities. *Energies, 13*(15), p. 3929.

Naef, T. (2023). *Concluding Remarks: Data Protection Without Data Protectionism.* In: Data Protection without Data Protectionism. European Yearbook of International Economic Law, vol 28. Springer, Cham., https://doi.org/10.1007/978-3-031-19893-9_6, p. 141-147.

Olawuyi, D.S. (2021) Local Content and Sustainable Development in Global Energy Markets. Treaty Implementation for Sustainable Development. Cambridge University Press, p. 42.

Papadopoulos, I., Gkonis, P. (2019) Personal Data Protection in the Energy Sector: An Analysis of the General Data Protection Regulation (GDPR) Provisions. Energy Policy 135, p. 1-10.

Partain, R., (2020) *Coordinating Public and Private Sustainability.* Green Energy Policy, International Trade Law, and Economic Mechanism. Routledge, Taylor and Francis, p. 32-34.

Richter, P., Bräuer, S. (2017) Data Protection in Smart Grids: An Overview of Risks and Countermeasures. *Computers & Security, 64*, p. 1-17.

Steinberg, J. K., Trubek, D.M. (2018) A Mixed-Methods Approach to Legal Research: Combining Empirical Methods with Normative Analysis. *Law and Social Inquiry, 43*(4), p. 1304-1337.

Svetlič, R., Krajcar, U. (2018) Legal Aspects of Cybersecurity and Data Protection in Slovenia's Energy Sector. *Central European Journal of Energy and Geoscience, 6*(1), p. 25-37

Takahashi, H. (2020) The Impact of the Proposed EU E-privacy Regulation on Energy Sector Digitization. *Renewable and Sustainable Energy Reviews, 125*, p. 1-9.

Van der Pas, J. W. G. (2020*) EU Data Protection Law and the Energy Sector.* In: Energy Law and Data Protection Law in the EU, edited by J. W. G. van der Pas and J. van der Weide. Springer, p. 232-256.

Vesel, T., Kresal, B. (2018) Cybersecurity and Data Protection in the Energy Sector: An Overview of Legal Issues in Slovenia. *Journal of Energy and Natural Resources Law, 36*(2), p. 183-203.

Wartusch, A., Zapf, K., (2020) The EU's Regulation on the Free Flow of Non-Personal Data and its Impact on the Energy Sector. *European Energy Journal, 10*(4), p. 16-22.

About the author

Zoran Dimović, University of Maribor, Faculty of Law, PhD in Law candidate, e-mail: zoran.dimovic@student.um.si, mobile +386 51 373 519