Bialystok Legal Studies
Białostockie Studia Prawnicze
2026 vol. 31 no. 1

sciendo

DOI: 10.15290/bsp.2026.31.01.10

Received: 21.06.2025
Accepted: 10.01.2026

Aleksandrs Potaičuks
Riga Graduate School of Law, Latvia
aleksandrs.potaicuks@rgsl.edu.lv
ORCID ID: 0009–0009–8795–2867

Commercial Registers as Administrative Databases: Balancing Public Accessibility and Privacy

Abstract: Countries develop various administrative databases in order to better perform governmental functions or to specifically influence certain civil relations or the behaviour of individuals. One particular and distinctive type of database containing personal data is commercial registers in Europe, which have a specific characteristic: they are accessible to the public and the data published has a binding nature. At the same time, this public accessibility of the personal data in commercial registers, especially with the increasing availability of digital technologies and their impact on society, can create a conflict with the privacy of the individuals included in these databases. This article first examines commercial registers as a form of public digitalisation, and then how the European Court of Justice, in its case law, balances the public accessibility which is an integral part of commercial registers with the right to privacy and data protection. In conclusion, the article generalises the lessons from the European Court of Justice case law and from legal scholarship that can be applied to preserve privacy, while the public accessibility of commercial registers is respected.

Keywords: databases, GDPR, privacy, proportionality of state measures, ReNEUAL model rules

Introduction

Countries develop various administrative databases (Lisičar & Jurić, 2024, p. 14) in order to better perform governmental functions or to specifically influence certain civil relations or the behaviour of individuals. In this regard, administrative databases and digitalisation are becoming increasingly important in the field of administrative law (Motzfeldt & Næsborg-Andersen, 2018, p. 138). In fact, the new ReNEUAL model rules on EU administrative procedure already include special provisions on

© 2026 Aleksandrs Potaičuks published by Sciendo. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

administrative databases, thus marking a new dimension for administrative law (Hofmann et al., 2014, p. 250).

One particular and distinctive type of database containing personal data is commercial registers in Europe, which, compared to other databases such as electronic health record systems or population registers, have a specific characteristic – they are publicly accessible and the data disclosed in them is binding. At the same time, this online availability of personal data and the public accessibility of commercial registers, especially with the increasing availability of digital technologies and their impact on society (Costa, 2023; Jabłoński, 2025, p. 162; Mazur & Ramiro Troitiño, 2024; Papacharissi & Gibson, 2011, p. 84), can create a conflict with the privacy of the individuals included in these databases. How can an individual claim their privacy given the public accessibility of commercial registers, and how can the balance of both be maintained?

The European Court of Justice (CJEU) has recently adopted at least four landmark judgments within a short period of time that balance data protection rights with the public accessibility that provides legal certainty in commercial registers; two more cases are still pending at the time of writing this article. As seen in one of the pending cases, the Constitutional Court of Latvia has also joined the debate, submitting another reference for a preliminary ruling on the protection of privacy in commercial registers (*Jautiva*, C-798/24).

This article employs a doctrinal research method centred on the analysis of CJEU case law relating to commercial registers in the European Union. While the research aim is to analyse the role of commercial registers and the principles established by the CJEU in its latest case law, the article raises a broader research question: how can transparency in commercial registers be balanced with privacy and data protection under European Union law in order to safeguard the fundamental rights of individuals? Thus, from a methodological point of view, this article focuses on the developments in CJEU case law and appraises the factors that controllers of commercial registers should take into consideration to avoid jeopardising fundamental rights, especially privacy and data protection.

While not denying the importance of public accessibility for commercial registers, in this paper I will examine commercial registers, as a form of public digitalisation, as well as existing CJEU case law to identify current data protection challenges and how the CJEU is shaping the GDPR. Firstly, in view of privacy concerns, I will analyse the special role of the commercial registers and the need for public accessibility. Secondly, I will present the leading cases concerning the intersection of privacy and commercial registers. Thirdly, I will generalise the lessons from the CJEU and demonstrate how the public accessibility of commercial registers is balanced with privacy in the age of public digitalisation and AI.

1. Commercial registers as administrative databases and their special role

Historically, commercial registers have evolved from the simple obligation to register a company and publish it in an official journal. Thus while historically, commercial registers used to be special books kept by commercial courts (Škorić, 2020, p. 3), today they are technologically advanced online databases containing a wealth of information for traders. Moreover, many public registers were in fact established and functioning long before data protection laws began to emerge (Lisičar & Jurić, 2024, p. 13).

In European countries, commercial registers are various (Heidemann, 2019, p. 19) and are operated and managed by very different public authorities: for example, in France and Germany there are authorised courts involved, whereas in Sweden, Denmark and Latvia there are agencies of a ministry. Today, however, the European Union has developed directives harmonising the rules for the creation and operation of a central register, commercial register or company register (hereinafter referred to as 'commercial registers') in the Member States (European Parliament & Council, 2017). Given the different nature of commercial registers, the focus of this research and the framework for the analysis of commercial registers as administrative databases is Directive (EU) 2017/1132 on certain aspects of company law.

Unlike many other administrative databases, such as population registers, electronic health record systems or criminal and law enforcement databases, commercial registers differ in specific features: firstly, information, including data on individuals, is not only stored for administrative purposes, but is also made available to the public; secondly, the information is not only publicly available, but also has a binding nature – it may be relied on by the company against third parties and thus provide legal certainty. Specifically, the purpose of disclosure of information in a commercial register is to protect the interests of third parties in relation to joint-stock and limited liability companies (Judgment of the CJEU, 2017), especially in situations where it is important to clarify who is authorised to bind the company (Judgment of the CJEU, 2024) or to assess good faith (Blajer, 2023, p. 114). The purpose of such disclosure is to enable any third person to inform themselves of these matters without having to establish a right or an interest to be protected (Judgment of the CJEU, 2017). Moreover, commercial registers differ from other types of administrative databases in that they are established in each Member State (de la Guardia, 2005). They therefore have a special role to play in improving trade between Member States and in creating the single market of the European Union (Judgments of the CJEU, 2017, 2024), especially as a form of digitisation (Ayata, 2024; Ferretti, 2022; Troitiño et al., 2024) or even the digital single market (Troitiño, 2022, p. 75). Registries and archives can also be seen as tools for developing the welfare state (Reichel & Chamberlain, 2021, p. 42).

The general standard for commercial registers as databases is that data may only be entered into a database for the legitimate purposes specified in the basic act (Hof-

mann et al., 2014, p. 250). Therefore the list of documents and particulars that must be disclosed by companies, kept by commercial registers and subsequently made available to the public is laid down by law (European Parliament & Council, 2017). This includes, for example, the instrument of constitution and statutes, the appointment, termination of office and particulars of the persons who are authorised to represent or take part in the administration, supervision or control of the company, the appointment of liquidators and particulars concerning them, etc. Currently in the European Union, in terms of the information to be disclosed to public, there is a dual approach: the EU legislation sets out the minimum information to be disclosed in order to harmonise the approach between Member States, while Member States' legislation may require more extensive disclosure of documents and particulars in their national laws (Judgment of the CJEU, 2024). This may also be relevant later when considering 'who is to blame' and the compatibility of the disclosure of personal data with the fundamental right to the protection of personal data and privacy, as some of these elements of information may or may not be considered personal data within the meaning of Article 4(1) of the GDPR (see section 2.1. on the notions of 'personal data' and 'processing' in the commercial register).

The information mentioned above, which is subject to compulsory disclosure in a commercial register and as such is made available to other businesses, is covered by public credibility (Gonet & Wolska, 2019, p. 86). Firstly, it is presumed that the data entered in public registers are true and consistent with actual and legal status (Gonet & Wolska, 2019, p. 86). Secondly, the commercial register's obligation to disclose information is closely related to the scope of information that is subject to statutory registration and storage by the commercial register (Judgment of the Supreme Court of Latvia, 2019). Thirdly, anyone who relies on publicly available register records which are subject to statutory disclosure must be presumed to be unaware of any existing inaccuracies contained in the records of the commercial register (Garnowski, 2022, p. 83). Thus the public credibility principle forms the cornerstone of commercial registers, and its most important effect is the promotion of legal certainty in commercial relations.

While the importance of such legal certainty is not contested, either historically or today, it is clearly evident that commercial registers have evolved from being special books kept by commercial courts into powerful digital databases, which puts much greater pressure on individuals' privacy. The increasing public accessibility, particularly influenced by technological advances such as search engines and artificial intelligence, forces us to look at public accessibility and privacy in a different light (Kerikmäe et al., 2019; Mokrá, 2023; Rek, 2024). Such reconsideration not only takes place in relation to databases; it also occurs more generally whenever any kind of information is published, including publicly available court judgments (Potaičuks & Tamužs, 2025, p. 5). It is important to bear in mind that the use of technology cannot happen at the expense of human rights or individual administrative rights. Therefore

it is important to strike a fair balance between, on the one hand, the specific objectives of the commercial register, and on the other, fundamental rights, especially privacy and data protection.

2. The scope of the right to private life covering entries in state administrative databases

2.1. The notions of 'personal data' and 'processing' in commercial registers

The next question is whether the fact that the data of private individuals related to a company are included (and processed) in a commercial register excludes these data from being classified as 'personal data' within the meaning of points 1 and 2 of Article 4 of the GDPR. There seems to be a misconception that all the data contained in a commercial register, including the persons who are authorised to represent the company or its liquidators, are considered to be data of the company, but are not 'personal data' as covered and protected by the GDPR. This seems to stem from Recital 14 of the GDPR, which states that 'this regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person' (European Parliament & Council, 2016).

While it is true that the GDPR does not cover data that clearly relates to legal persons, including their name, form of registration and contact details (van der Sloot, 2015, p. 40), this cannot be overgeneralised in relation to all entries. The notions of 'personal data' and 'processing' were intentionally worded broadly and non-exhaustively in the GDPR and its preceding directive (Outeda, 2024; Purtova, 2018, p. 41). Data such as the name, contact details, etc., of natural persons representing a legal person are provided to a commercial register in the course of professional activity and normally fall within the wording of the definition of 'personal data' within the meaning of point 1 of Article 4 of the GDPR. Such an activity (provision of data to and storage in the commercial register, as well as disclosure) does not generally fall outside the scope of the GDPR, as defined in Article 2(2).

In this instance, the CJEU has ruled that 'the disclosure of the name, surname and contact details of natural persons representing a legal person falls within the meaning of point 1 of Article 4 of the GDPR' and 'this interpretation cannot be invalidated by recital 14 of the GDPR. The second sentence of that recital refers, inter alia, to the "name" and "contact details" of the legal person, and not that of the natural persons acting in the name of or on behalf of a legal person' (Judgment of the CJEU, 2025). Thus according to the CJEU, the disclosure of the data of natural individuals in this situation does indeed constitute the processing of 'personal data' (Judgments of the CJEU, 2017, 2024, 2025), and the fact that the disclosure is made for the purpose of the identification of the representation of the legal person is irrelevant (Judgment

of the CJEU, 2024). In this context, Article 161 of Directive 2017/1132 on company law and commercial registers also explicitly states that '[t]he processing of personal data carried out in the context of this Directive shall be subject to Directive 95/46/EC', and thus to the GDPR as well.

2.2. Direct and indirect disclosure of personal data in commercial registers

Disclosure of personal data in commercial registers can occur directly, when the personal data elements are the records themselves, or indirectly, when personal data is included in submitted documents and disclosed as part of a unit. Specifically, as seen in the case law, some particulars are 'disclosed directly', such as the names of persons who are authorised to represent or take part in the administration, and can be classified as personal data, whereas some particulars qualifying as personal data may be 'disclosed indirectly' (Judgment of the CJEU, 2024), such as the disclosure of the instrument of constitution or statutes (document) containing the names of the persons, their passport data or their signature (Judgment of the CJEU, 2024). In the latter situation, it is important to consider whether the personal data disclosed by the company can be qualified as subject to mandatory disclosure (and has a statutory basis requiring disclosure), complies with the data minimisation principle of the GDPR and is thus covered by the 'public credibility' principle.

3. Clashes between two competing interests: Public accessibility and the protection of privacy

Although commercial registers have been around for a while, the CJEU has in a short period of time received a number of preliminary rulings from Member States where public access to information has clashed with privacy and data protection. While case law shows that the rules on the protection of personal data do not prevent commercial registers from being subject to a fully open access regime (Lisičar & Jurić, 2024, p. 27), registers are still subject to specific measures that must be taken into account in order to balance data protection concerns. On its way from *Manni* to *Ministerstvo zdravotnictví*, the CJEU has provided significant clarification on the protection of personal data related to commercial registers and companies.

3.1. Manni (C-398/15): On the public availability of historical data in the commercial register

In *Manni*, the applicant objected to his personal data being accessible to the public in the commercial register 15 years after his former company had been declared insolvent and struck off the company register. The applicant alleged that the public availability of such historical data adversely affected his current business affairs, and requested the erasure of personal data relating to him in the commercial register. Thus this case showed the challenge of whether the former data protection directive

(now the GDPR) and the directive on the disclosure of company documents preclude a situation where any member of the public has access to data relating to natural persons contained in the commercial registers, without any time limit, and how public accessibility, the right to be forgotten and the principle of storage limitation are manifested in commercial registers (Judgment of the CJEU, 2017).

3.2. Luxembourg Business Registers (C-37/20): On the public accessibility of information on the beneficial ownership of companies

In *Luxembourg Business Registers*, due to anti-money laundering legislation, the applicant's data were made available in the commercial register to any member of the public, but the applicant wanted his personal data on the beneficial ownership to be restricted to a narrower public rather than available to anyone. The applicant argued that public access to his information could expose him and his family to 'a disproportionate risk of fraud, kidnapping, blackmail, extortion, violence and intimidation'. Thus this case raised the issue of the validity of the EU provision whereby information on the beneficial ownership of companies is made accessible in all cases to any member of the general public, incompatibly with the right to respect for private life and the protection of personal data as enshrined in the Charter of Fundamental Rights (the Charter) (Judgment of the CJEU, 2022).

3.3. Agentsia po vpisvaniyata (C-200/23): On the competence of a commercial register to erase personal data in the constitutive instrument of a company

In *Agentsia po vpisvaniyata*, after the founding of the company and the submission of the constitutive instrument to the commercial register, the personal data of the applicant contained in the constitutive instrument (including their surname, first name, ID number, ID card number, date and place of issue of that card, and the applicant's address and signature) were made available to the public through the register. The applicant requested the commercial register to erase the personal data from the publicly available constitutive instrument. However, the commercial register took the view that it is the applicant who must submit an authenticated copy of the constitutive instrument in which the personal data of the company members (other than the personal data required by law) were properly redacted, but the register itself was not able to edit personal data. Thus this case highlighted the challenge of whether national laws can prevent or restrict the erasure of personal data and how authorities maintaining commercial registers should comply with the 'right to erasure' procedures in commercial registers (Judgment of the CJEU, 2024).

3.4. Ministerstvo zdravotnictví (C-710/23): On whether the data relating to legal persons may be personal data

The dispute in *Ministerstvo zdravotnictví* concerns the individual's public access to official documents. A member of the public requested the Ministry of Health to provide information about a public purchase agreement, specifically the parties signing this agreement. Even though the Ministry provided the requested information, it redacted personal data from the issued documents, including the names, signatures, positions, and contact information of natural persons representing legal entities. Thus this case raised the question of whether information about natural persons representing legal entities constitutes personal data under the GDPR if it is used solely to identify legal entities (Judgment of the CJEU, 2025).

3.5. Pending cases: Jautiva (C-798/24) and Unione Fiduciaria (C-685/24)

In both *Jautiva* and *Unione Fiduciaria*, the national courts of Latvia and Italy referred the question to the CJEU to clarify whether the data required to be disclosed in the commercial registers to any member of the general public under national law – every shareholder of a joint-stock company in Latvia (*Jautiva*) and beneficial owners of trusts and similar legal arrangements in Italy (*Unione Fiduciaria*) – fall within the scope of information to be disclosed to the public in the light of existing European Union legislation on the protection of personal data. Neither case has yet been adjudicated.

4. Balancing public accessibility and privacy in the context of commercial registers

4.1. The scope of the right to private life and data protection covering entries in commercial registers

The analysis of the above-mentioned court cases shows that the disclosure of personal data (with online availability) in the commercial registers (which is required by law), in a way that makes the personal data available in all cases to any member of the general public, methodologically constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. However, where such disclosure is ordered by national laws, it can constitute an interference under national constitutions as well and thus be deemed unconstitutional at a national level (Šulmane, 2025, p. 304).

Before registers were made accessible online, anyone wanting to receive data from a register would typically have had to visit the institution that controlled it and request the data in person (Lisičar & Jurić, 2024, p. 25). However, the online availability of data has changed people's habits and the extent to which privacy is impacted.

The CJEU in this regard has even considered that such online availability of, for example, beneficial ownership information constitutes 'a serious interference' (Judgment of the CJEU, 2022; Lisičar & Jurić, 2024, p. 24). This is due to the facts that (1) such information can be used to create a profile of the state of the person's wealth, investment choices, etc.; (2) online availability to a wide audience also gives access to people who, for reasons unrelated to the objective of the measure, may be able to find out about the material and financial situation of the data subject; and (3) similar to the Latin expression 'verbum semel emissum volat irrevocabile', once personal data are publicly disclosed by the register, it is extremely difficult to control successive processing, and thus the data subjects are unable to defend themselves against abuse (Judgment of the CJEU, 2022).

However, the fact that there is an interference with the fundamental right does not automatically lead to a violation of it, since, according to the case law and Article 52(1) of the Charter, Articles 7 and 8 of the Charter are not absolute and interference can be justified, considering these rights in relation to their function in the society (Judgment of the CJEU, 2022; Mudrecki, 2021, p. 41).

4.2. Balancing interests: A method of evaluating the justification for interference

For any limitation on the exercise of a fundamental right (including the right to privacy and data protection when personal data are disclosed to the public) to be considered justified, it must, firstly, be provided for by law; secondly, must respect the essence of those rights; thirdly, must meet objectives of general interest recognised by the EU; and fourthly, must be appropriate, necessary and proportionate. In the current case law, the strongest clashes between privacy and public accessibility in relation to commercial registers seem to occur mainly at the level of the third and fourth of these criteria. Consequently, the following sub-sections will first explain the most important conclusions of the judgments in relation to commercial registers, and will then provide a deeper analysis of the 'objectives of general interest' and 'appropriate, necessary and proportionate' criteria, which balance public accessibility and privacy.

4.3. Lessons for commercial registers: From Manni to Ministerstvo zdravotnictví

In *Manni* (on the right to be forgotten (Vardanyan et al., 2023, p. 97) in a commercial register after expiry of a sufficiently long period after the dissolution of a company), the CJEU was seemingly faced with a Gordian knot: the absence of heterogeneity in the limitation periods provided for in national laws and thus the impossibility of claiming that personal data are no longer necessary in a commercial register. While the CJEU acknowledged that storing personal data for longer than necessary could be problematic in terms of proportionality, it was nevertheless accepted that the impossibility of erasing personal data did not result in disproportionate interference, as the need to pro-

tect third parties and fair trading took precedence. This case has been criticised in legal scholarship for denying the right to be forgotten (Caravà, 2017, p. 292).

However, in *Luxembourg Business Registers* (on publishing the beneficial ownership of companies), the CJEU took a much restrictive approach and held that the disclosure of personal data on beneficial owners in the register was neither limited to what was strictly necessary nor proportionate to the objective pursued. This was especially the case because the provisions allowed disclosure of personal data which were not sufficiently defined and identifiable in these provisions; in addition, some optional provisions allowed the disclosure of personal data on condition of online registration, but were not in themselves able to demonstrate a proper balance or the existence of sufficient safeguards against the risk of abuse. In other words, the CJEU considered that the difficulty in defining the cases and conditions under which the general public can access information on beneficial owners could not justify the legislature's decision to grant access to the public as a whole (Cindori, 2023, p. 125). Such insufficient regulation can also lead to violation of the fundamental principles of administrative functioning (Štemberger Brizani, 2024, p. 162; Wegner, 2025, p. 28).

While in *Manni*, the CJEU held that it is proportionate to refuse to erase personal data in a commercial register after a company has ceased to exist, in *Agentsia po vpisvaniyata*, it took a different view. Specifically, faced with the situation that the register disclosed personal data not specifically and strictly required by law, the CJEU considered that this does not satisfy the 'necessity' requirement: it does not serve the objective of general interest and as such does not strike a fair balance between those objectives and data protection rights (Judgment of the CJEU, 2024). Another element criticised by the CJEU was the alleged lack of the Member State's administrative power to delete personal data. The CJEU ruled against the breach of the principle of prohibition of legal obstruction by institutions: the authority, in order to justify not erasing personal data, insisted that it does not review particulars (the personal data contained in the electronic images or originals of documents submitted to it), which were subject to a compulsory disclosure under Directive 2017/1132, before they are made available online, and therefore does not have the competence to erase anything. However, the CJEU ruled that the authority is the controller of the personal data and therefore is responsible for compliance with paragraph 1 of Article 5(2) of the GDPR (Judgment of the CJEU, 2024).

While in *Luxembourg Business Registers*, concerning personal data disclosed by private companies in a commercial register, the principle of transparency was not accepted by the CJEU as a justification, *Ministerstvo zdravotnictví* concerned public access to official documents in a public authority (not in a register). Therefore the principle of transparency was applicable and played a different and decisive role in balancing privacy. The CJEU held that, unlike in the case of commercial registers, there was a balancing of different interests: the public interest in scrutinising the public administration (Judgment of the CJEU, 2022) versus the right to protection of per-

sonal data. However, the problematic core identified in this context was the principle of proportionality: while Member States have the power to introduce national provisions to further specify data protection rules (Hamuľák, 2016; Maatsch, 2024), they also must ensure that the practical consequences, in particular of an organisational nature, arising from the additional requirements which they have laid down are not excessive (Judgment of the CJEU, 2025).

4.4. The 'objectives of general interest' criterion

In relation to the criterion of the 'objectives of general interest as recognised by the EU', the disclosure of personal data in commercial registers may serve various objectives, depending on the nature of the data. As identified in *Manni*, the objective can be the protection of third parties who are dealing with a company, in particular to identify the person authorised to bind the company. In *Luxembourg Business Registers*, it was identified that the data of beneficial owners may serve the objective of preventing money laundering and terrorist financing by creating, through increased transparency, an environment less likely to be used for these purposes. However, these objectives cannot be overgeneralised; each legal norm relating to the disclosure of certain elements or groups of personal data must have a specific objective of general interest. Additionally, in this context, the data subject must be able to reasonably expect their personal data to be processed for particular purposes (Jekabsone, 2023, p. 54). However, even though disclosing personal data in a register serves a specific objective of general interest, the possibility of using the data for purposes not envisaged by the legislation is an inherent risk of every public register (Lisičar & Jurić, 2024, p. 25).

Moreover, in this context, it is important to draw a red line between the public accessibility of activities of a public or of a private nature, such as the disclosure of company data in commercial registers. The general principle of transparency enshrined in Articles 1 and 10 TEU and Article 15 TFEU specifically covers activities of a public nature, such as the use of public funds, the work of public institutions, etc. By contrast, the information regarding the work of private companies, including their beneficial owners, is a distinct activity. Therefore, as established by case law, the principle of transparency as such cannot be considered an objective of general interest capable of justifying the interference which results from the general public's access to personal data held and disclosed by private companies in a commercial register (Judgment of the CJEU, 2022).

4.5. The 'appropriate, necessary and proportionate' criterion

Under the 'appropriate, necessary and proportionate' criterion, it is essential to examine, firstly, whether public access to information is appropriate for achieving the pursued objective of general interest; secondly, whether the interference with the fundamental rights resulting from such access is limited to what is strictly nec-

essary (in the sense that the objective could not reasonably be achieved as effectively by other means less prejudicial to the fundamental rights of the data subjects); and thirdly, whether that interference is not disproportionate to that objective, which implies in particular a balancing of the importance of the objective and the seriousness of the interference (Judgment of the CJEU, 2022).

- The following aspects have been relevant in case law so far when assessing the appropriateness, necessity and proportionality of personal data in a commercial register:
- The set of data made available is limited, clearly and exhaustively defined, and must be of a general nature in order to minimise potential prejudice (Judgments of the CJEU, 2017, 2022, 2025);
- Personal data is not stored longer than necessary (Judgment of the CJEU, 2017);
- There is opportunity to have derogation from disclosure in 'exceptional circumstances', on a case-by-case basis (Judgments of the CJEU, 2017, 2022);
- There is an absence of administrative restraints in compliance with the principles relating to the processing of personal data, such as the lack of competence of public authorities to erase personal data (Judgment of the CJEU, 2024);
- Personal data is provided on the condition of online registration in order to identify the person requesting that information (Judgment of the CJEU, 2022);
- Information is made available to the whole of society, even though the control of the matter is reserved to the competent authorities, and therefore these authorities or obligated entities should have access to personal data instead (Judgment of the CJEU, 2022);
- There is an absence of excessive national practical arrangements that undermine the content and objectives of data protection (Judgment of the CJEU, 2025).

While these aspects are relevant to commercial registers, this list, firstly, is by no means exhaustive, and, secondly, each aspect on its own is unlikely to undermine the 'appropriate, necessary and proportionate' criterion. Instead, compliance with it must be assessed on a case-by-case basis, and a higher risk exists when several of the above aspects have a cumulative effect. Also, while these aspects were analysed in the case law, new technology should be considered in the context of its dynamic nature and the potential for it to offer measures that cause less harm to privacy. While technology is generally seen as endangering privacy, the literature suggests that such technologies can also be used to protect it; these are known as 'privacy-preserving technolo-

gies' (Timan & Mann, 2021, p. 159). In the case of commercial registers, where data (including personal data) are available to any member of the general public, artificial intelligence can potentially be used for smart access control or risk-based data disclosure; for example, it could evaluate data requests and determine the level of detail that individuals should be allowed to access. This would provide all the information necessary for the objectives of general interest without full-scale public accessibility, thus balancing privacy rights. Currently, there is also a call in the legal literature for new, third-generation commercial registers that could automate more state functions and use more next-generation LegalTech solutions (Szostek et al., 2025, p. 182).

Once such privacy-preserving technologies are available, the case law relating to the 'appropriate, necessary and proportionate' criterion will need to be reconsidered, as the existence of these technologies means that the objective could reasonably be achieved effectively through other, less prejudicial means, with the available modern privacy-preserving technologies. Up to now, the CJEU has not examined the concept of privacy-preserving technologies under the 'appropriate, necessary and proportionate' criterion.

Conclusions

As was anticipated in the introduction of this article, the research shows that the CJEU has provided clear factors that controllers of commercial registers should take into consideration to avoid jeopardising fundamental rights, particularly with regard to privacy and data protection. The analysis of case law shows that while every dispute relating to commercial registers is at its core different, the CJEU has developed a general methodological approach to balancing public accessibility and privacy in such registers. Firstly, in these cases, the public accessibility that is considered an integral part of commercial registers is, from a methodological perspective, seen as an interference with the privacy of the individuals included in them. Secondly, all elements of the public accessibility of personal data must serve a clear objective of general interest, and consequently comply with different considerations of 'appropriateness, necessity and proportionality'. Thus, as claimed in the introduction, CJEU case law envisions that behind the public accessibility of commercial registers, individuals are entitled to claim their privacy.

Firstly, specifically in the case of commercial registers as administrative databases, it is important to underline that the general principle of transparency enshrined in Articles 1 and 10 TEU and Article 15 TFEU cannot be considered an objective of general interest capable of justifying the interference which results from the general public's access to personal data held and disclosed by private companies in a commercial register. While this principle covers public activities, such as the use of public funds, a declaration of private interests by officials in public positions or the

work of public institutions, it cannot be applied equally to commercial registers and information regarding the work of private companies.

Secondly, the case law on commercial registers is clear: the Achilles heel in such cases is typically the failure to consider whether it is 'appropriate, necessary and proportionate' (Potaičuks, 2024, p. 84) to make different elements of personal data subject to public accessibility in specific circumstances. In generalising the above-mentioned failures to balance privacy, two directions can be distinguished: the first serves to answer the question 'What is subject to public accessibility?', while the second addresses the question 'How is it subjected to public accessibility?' To be precise, the first direction is related to the type and extent of personal data in relation to the objective of general interest, while the second direction relates to the measures that minimise privacy damage or serve as a precautionary measure in relation to public accessibility. Examples of such measures include the opportunity to request derogation in 'exceptional circumstances', the activity of national authorities that minimises the negative impact on privacy, limitations on storage and the use of alternative technological solutions, such as online registration.

Commercial registers have come a long way. They have evolved from paper-based books kept by commercial courts that had to be visited in person to request data to powerful databases with lots of information available publicly online, thus causing new concerns and putting privacy under pressure. While public accessibility is an inherent feature of commercial registers today, the possibility of using this accessibility and the data they contain for purposes not envisaged by legislation is an inherent risk for every public register as well. This is an area in which privacy-preserving technologies, especially those offered by new AI-based opportunities, could transform the concept of public accessibility and balance the risks to privacy posed by it.

REFERENCES

Ayata, Z. (2024). European Union contracts in digital environments. In D.R. Troitiño (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 173–185). Springer Nature Switzerland.

Blajer, P. (2023). On the principle of public faith of land registers in a comparative context. *European Property Law Journal*, 12 (2–3), 79–125. https://doi.org/10.1515/eplj-2023–0005.

Caravà, E. (2017). Personal data kept in companies registers: The denial of the 'right to be forgotten'. *European Data Protection Law Review*, *3*(1), 287–292. https://doi.org/10.21552/edpl/2017/2/26

Cindori, S. (2023). Beneficial ownership – Demand for transparency, threat to privacy. *Review of European and Comparative Law*, *55*(4), 113–131. https://doi.org/10.31743/recl.16352

Costa, M. I. (2023). The legal concept of discrimination by association: Where does it fit into the digital era? *UNIO–EU Law Journal*, *9*(1), 16–28.

de la Guardia, R. M. (2005). La política europea de España después de su integración en las Comunidades. *Cuadernos europeos de Deusto*, *32*, 61–84.

European Parliament and Council. (2016, 27 April). On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (O. J. L 119, 04.05.2016).

European Parliament and Council. (2017, 14 June). Directive (EU) 2017/1132 of the European Parliament and of the Council Relating to Certain Aspects of Company Law (Codification) (O. J. L 169, 30.06.2017).

European Union. (2007, 12 December). Charter of Fundamental Rights of the European Union (O. J. C 326, 26.10.2012).

Ferretti, F. (2022). A single European data space and data act for the digital single market: On datafication and the viability of a PSD2-like access regime for the platform economy. *European Journal of Legal Studies*, *14*, 173–218s.

Galetta, D.U., Hofmann, H. C. H., Lottini, M., Marsch, N., Schneider, J. P., Tidghi, M. (2014). Book VI – Administrative Information Management. In H. Hofmann, J. P. Schneider, & J. Ziller (Eds.). *ReNEUAL model rules on EU administrative procedure* (pp. 232–318). ReNEUAL research network on EU administrative law. https://hdl.handle.net/10993/19862

Garnowski, K. (2022). The principle of reliability of business trading in the context of personal changes in partnerships. *Review of European and Comparative Law 51*(4), 79–94. https://doi.org/10.31743/recl.14603

Gonet, W., & Wolska, H. (2019). Performing legal transactions based on entries in public registers: Selected issues. *Journal of Management and Financial Sciences*, *36*(1), 85–101. https://doi.org/10.33119/JMFS.2019.36.6

Hamuľák, O. (2016). *National sovereignty in the European Union: View from the Czech perspective*. Springer.

Heidemann, M. (2019). Commercial registers and transparency. *Amicus Curiae*, *112*(2017), 18–24. https://doi.org/10.14296/ac.v2017i112.5042

Jabłoński, M. (2025). The right to privacy and the obligation to transfer and authenticate personal data through the internet: Conflicting issues. *Bialystok Legal Studies*, *30*(4), 161–175. https://doi.org/10.15290/bsp.2025.30.04.10

Jekabsone, I. (2023). Selected legal issues in online adult education: Compliance of online learning and teaching process with GDPR. *TalTech Journal of European Studies*, *13*(2), 46–62. https://doi.org/10.2478/bjes-2023–0015

Judgment of the CJEU of 9 March 2017 on the case of *Manni*, C-398/15, ECLI:EU:C:2017:197.

Judgment of the CJEU of 22 November 2022 on the case of *Luxembourg Business Registers*, joined cases C-37/20 and C-601/20, ECLI:EU:C:2022:912.

Judgment of the CJEU of 4 October 2024 on the case of *Agentsia po vpisvaniyata*, C-200/23, ECLI:EU:C:2024:827.

Judgment of the CJEU of 3 April 2025 on the case of *Ministerstvo zdravotnictví*, C-710/23, ECLI:EU:C:2025:231.

Judgment of the Supreme Court of Latvia of 31 January 2019 in case no. SKA 148/2019 (A420322015).

Lisičar, H., & Jurić, M. (2024). How much transparency is too much? Open access to public registers in Croatia and personal data protection. *SEE Law Journal*, *13*(1), 12–31.

Kerikmäe, T., Troitiño, D. R., & Shumilo, O. (2019). An idol or an ideal? A case study of Estonian e-governance: Public perceptions, myths and misbeliefs. *Acta Baltica Historiae et Philosophiae Scientiarum*, *7*(1), 71–80.

Maatsch, A. (2024). Parliamentary adjustment during a crisis: Interplay of digitalization and domestic context factors. *Internet of Things*, *27*, 101316.

Mazur, V., & Ramiro Troitiño, D. (2024). The members of the EU and e-governance, analysis, and institutional support. In D.R. Troitiño (Ed.), *E-Governance in the European Union: Strategies, tools, and implementation* (pp. 39–55). Springer Nature Switzerland.

Mokrá, L. (2023). Digitally sovereign individuals: The right to disconnect as a new challenge for European legislation in the context of building the EU digital market. In D. R. Troitiño, T. Kerikmäe, O. Hamuľák (Eds.), *Digital development of the European Union: An interdisciplinary perspective* (pp. 189–197). Springer International Publishing.

Motzfeldt, H. M., & Næsborg-Andersen, A. (2018). Developing administrative law into handling the challenges of digital government in Denmark. *Electronic Journal of e-Government*, *16*(2), 136–146.

Mudrecki, A. (2021). The contemporary significance of the principle of proportionality in tax law. *Bialystok Legal Studies*, *26*(4), 37–51, https://doi.org/10.15290/bsp.2021.26.04.03

Outeda, C. C. (2024). The EU's AI Act: A framework for collaborative governance. *Internet of Things*, 27 (01291).

Papacharissi, Z., & Gibson, P. L. (2011). Fifteen minutes of privacy: Privacy, sociality, and publicity on social network sites. In S. Trepte, L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 75–89). Springer Berlin Heidelberg.

Potaičuks, A. (2024). Data protection under review of constitutional court: Administrative databases directly accessible to public authorities. *TalTech Journal of European Studies*, *14*(2), 73–87. https://doi.org/10.2478/bjes-2024–0017

Potaičuks, A., & Tamužs, K. (2025). Open court principle and respecting privacy: Granting anonymity and restricting access to case files in constitutional court review procedure. *International Journal for Court Administration*, *16*(1), 1–14. https://doi.org/10.36745/ijca.593

Purtova, N. (2018). The law of everything: Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40–81. https://doi:10.1080/17579961.2018.1452176

Reichel, J., & Chamberlain, J. (2021). Public registries as tools for realising the Swedish welfare state: Can the state still be trusted? *Public Governance, Administration and Finances Law Review*, *6*(2), 35–52. https://doi.org/10.53116/pgaflr.2021.2.4

Rek, M. (2024). E-democracy in the EU. In D.R. Troitiño (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 103–115). Springer Nature Switzerland.

Škorić, S. (2020). The application of digital technology in business registration. *Pravo – teorija i praksa*, *37*, 1–12. https://doi.org/10.5937/ptp2004001S

Štemberger Brizani, K. (2024). Administrative contract in administrative matters: Slovenian law in comparative perspective. *Bratislava Law Review*, *8*(1), 153–168. https://doi.org/10.46282/blr.2024.8.1.717

Šulmane, D. (2025). Defense concept through the legislature – Protecting values for the sustainability of society. *Environment Technology Resources: Proceedings of the 16th International Scientific and Practical Conference*, *5*, 303–309. https://doi.org/10.17770/etr2025vol5.8511

Szostek, S., Malarewicz-Jakubów, A., & Castellani, M. (2025). Koncepcja i podstawy prawne dla nowego ujęcia rejestru – Rejestr 3.0. *Bialystok Legal Studies*, *30*(3), 181–195. https://doi.org/10.15290/bsp.2025.30.03.12

Timan, T., & Mann, Z. (2021). Data protection in the era of artificial intelligence: Trends, existing solutions and recommendations for privacy-preserving technologies. In E. Curry, A. Metzger, S. Zillner, J. C. Pazzaglia, A. García Robles (Eds.), *The elements of big data value: Foundations of the research and innovation ecosystem* (pp. 153–175). Springer International Publishing.

Troitiño, D. R. (2022). The European Union facing the 21st century: The digital revolution. *TalTech Journal of European Studies*, *12*(1), 60–78. https://doi.org/10.2478/bjes-2022–0003

Troitiño, D. R., Mazur, V., & Kerikmäe, T. (2024). E-governance and integration in the European Union. *Internet of Things*, *27*(1), 101321. https://doi.org/10.1016/j.iot.2024.101321

van der Sloot, B. (2015). Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system. *Computer Law & Security Review*, *31*(1), 26–45. https://doi.org/10.1016/j.clsr.2014.11.002

Vardanyan, L., Kocharyan, H., Hamulák, O., Mesarčík, M., Kerikmäe, T., & Kookmaa, T. (2023). The unwanted paradoxes of the right to be forgotten. *Masaryk University Journal of Law and Technology*, *17*(1), 87–109.

Wegner, J. (2025). The constitutionalization of the internet and the right to non-use. *Bialystok Legal Studies*, *30*(4), 28. https://doi.org/10.15290/bsp.2025.30.04.02