sciendo

Ius Novum

2025, vol. 19, no. 4, pp. 175–189

DIGITAL PROCESSES IN EU COMPANY REGULATIONS AND THEIR IMPLICATIONS FOR REGISTRY PRACTICES

TOMASZ BRAUN*

DOI 10.2478/in-2025-0043

Abstract

This paper examines the impact of European Union law on digitalisation, considering both its foundations and effects. Some of these aspects are addressed in Directive (EU) 2017/1132 of the European Parliament and of the Council on certain aspects of company law, as well as in the Directive of the European Parliament and of the Council amending Directives 2009/102/EC and (EU) 2017/1132 as regards further expanding and upgrading the use of digital tools and processes in company law. As a consequence of these legislative developments, several issues have since emerged. Examples include difficulties related to the online registration of companies introduced by Member States following the implementation of the Directive, and discrepancies between the information contained in national central business registers interconnected within the Business Registers Interconnection System (BRIS). In this context, the paper analyses the implications of the Court of Justice of the European Union's judgment in the *Manni* case and explains why the 'right to be forgotten' may not apply in this area. Another issue arising from digitalisation concerns trust services, including the work of notaries and their relationship with Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation), as well as Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. On this occasion, the paper also discusses why the eIDAS Regulation may not necessarily have a harmonising effect across

* LLD, Lazarski University in Warsaw (Poland), e-mail: tomasz.braun@lazarski.edu.pl, ORCID: 0000-0003-0141-4929

the various legal systems within the EU. Finally, in light of the Fifth Anti-Money Laundering Directive of the European Union, the paper considers the concept of beneficial ownership, its notarial determination, and its relevance to the prevention of money laundering.

Keywords: registration of companies; digitalisation; EU; EU law; CJEU; business; company law; company registers; BRIS; interconnection of business registers; *Manni* case; right to be forgotten; data protection; disclosure; notary; eIDAS; beneficial owner

INTRODUCTION

Digitalisation is an unstoppable process that directly affects all business operations.[1] The global pandemic has accelerated these developments in an unprecedented manner. As a result, part of companies' commercial activities is now supported or even replaced by digital technologies. Digitalisation in law is an area of transformation that has been relatively broadly conceptualised in the literature.[2] The main subject of this paper is the examination of developments in European Union company law, which has recently undergone instrumental changes. These changes refer, inter alia, to Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 and 29 March 2023 relating to certain aspects of company law (codification, text with EEA relevance, hereinafter referred to as 'the Directive'). The rationale underlying this Directive lies in the fact that, until its adoption, the preceding directives concerning related matters had often been amended and revised. Work on the codification began in 2012 and eventually led to the harmonisation of several practical aspects related to the digitalisation of company law processes. The Directive entered into force on 20 July 2017.[3] Hence, the Directive incorporates the essence of several earlier directives:

1. Eleventh Council Directive 89/666/EEC of 21 December 1989 concerning disclosure requirements in respect of branches opened in a Member State by certain types of companies governed by the law of another State;[4]
2. Directive 2011/35/EU of the European Parliament and of the Council of 5 April 2011 concerning mergers of public limited liability companies (codification) (Text with EEA relevance);[5]

---

[1] See also the definition of digitalisation provided by Ž. Bregeš, T. Jakupak, 'Digitalization of business register', *InterEULawEast*, 2017, Vol. IV, Issue 2, p. 5: 'The term "digitalization" is the representation of communication in writing or sound by electronic means, and the concept thus concerns electronic communication, including the transmission of information and the storage of such communication electronically, as well as electronic access to and retrieval from such storage.'

[2] J.C. Llopis Benlloch, 'Notaries and digitalisation of company law', *ERA Forum*, 2018, Vol. 19, p. 52.

[3] Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (codification) (Text with EEA relevance) (OJ L 169, 30.6.2017); and Directive of the European Parliament and of the Council amending Directives 2009/102/EC and (EU) 2017/1132 as regards further expanding and upgrading the use of digital tools and processes in company law (COM(2023) 177 final, 2023/0089(COD)).

[4] OJ L 395, 30.12.1989.

[5] OJ L 110, 29.4.2011.

3. Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent (codified version) (Text with EEA relevance);[6]
4. Directive 2012/30/EU of the European Parliament and of the Council of 25 October 2012 on coordination of safeguards which, for the protection of the interests of members and others, are required by Member States of companies within the meaning of the second paragraph of Article 54 of the Treaty on the Functioning of the European Union, in respect of the formation of public limited liability companies and the maintenance and alteration of their capital, with a view to making such safeguards equivalent (recast) (Text with EEA relevance);[7]
5. Directive 2005/56/EC of the European Parliament and of the Council of 26 October 2005 on cross-border mergers of limited liability companies (Text with EEA relevance);[8]
6. Sixth Council Directive 82/891/EEC of 17 December 1982 based on Article 54(3)(g) of the Treaty, concerning the division of public limited liability companies.[9]

Consequently, the Directive replaced all six of these directives. The rationale for its implementation is regarded as, to some extent, political, being closely linked to the Digital Single Market Strategy.[10] Extensive explanations were provided in the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, as well as in the 2016 e-Government Action Plan and subsequent documents.[11] The Commission was encouraged by the Parliament to pursue digitalisation.[12] This particularly concerns the registration of companies and, thus, the life cycle of a company, which is closely connected with the realisation of rights deriving from the fundamental freedoms upon which the EU is founded.[13]

---

[6] OJ L 258, 1.10.2009.

[7] OJ L 315, 14.11.2012.

[8] OJ L 310, 25.11.2005.

[9] OJ L 378, 31.12.1982.

[10] See S. Omlor, 'Digitalization and EU Company Law, Innovation and Tradition in Tandem', *European Company Law*, 2018, p. 3; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3258980 [accessed on 29 December 2022].

[11] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Single Market Strategy for Europe*, COM(2015) 192 final; and European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – EU eGovernment Action Plan 2016–2020*, COM(2016) 179 final.

[12] See European Parliament, Resolution of 16 May 2017 on the EU eGovernment Action Plan 2016–2020 (2016/2273(INI)), OJ C307/2 and the Council Conclusions on Single Market Policy, 6197/15, 2–3 March 2015.

[13] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Commission Work Programme 2017. Delivering a Europe that protects, empowers and defends*, COM(2016) 710 final, p. 9. However, the idea was closely connected with the Commission's FinTech Action Plan.

ONLINE REGISTRATION OF COMPANIES AND THE INTERCONNECTION OF BUSINESS REGISTERS (BRIS)

Pursuant to the provisions of the Directive, each Member State enables the online registration of companies. Directive (EU) 2017/1132 formally applies to both single-member and multi-member companies.[14] However, it also refers to natural persons and legal entities.[15] Such registration is intended to provide a simplified form of company incorporation and does not require a notarial deed, as is normally the case in some Member States. The process of company registration consists of entering the relevant information on a dedicated website. Business registers are administered by public authorities: for instance, in Denmark by the Danish Business Authority (Virk); in Poland by the Ministry of Justice; and in the United Kingdom (despite Brexit) by Companies House, the government's official register of companies. Online registration procedures have indeed proved to be both time- and cost-efficient,[16] responding effectively to the needs of a rapidly changing and increasingly digital business environment. When registering a company online, it is required to provide:[17]

- a shareholders' agreement (charter) establishing the company,
- information on the required minimum share capital,
- the registered name,
- contact details,
- the relevant registry court at the company's seat, and
- a list of shareholders, members of the company's management bodies, and its branches.

Directive (EU) 2017/1132 provides for the creation of a system interconnecting company registers.[18] This system serves as a universal European central platform[19] composed of the Member States' registers, functioning as an electronic access point.[20] Member States are obliged to ensure the compatibility and interoperability of their

---

[14] Nevertheless, in doctrine, it is also suggested that multi-member companies could be excluded from the Directive applicability (see S. Omlor, 'Digitalization…', op. cit., p. 6; and T. Wachter, 'Neues zum Europäischen Gesellschaftsrecht: Digitalisierung im GmbH-Recht (I)', *GmbH-StB*, 2018, No. 7, pp. 218–219.

[15] Pursuant to Article 13 of the Directive, with regard to company registers, the Directive is applicable to companies listed in Annex II of the Directive. For instance, in Germany this would be *die Gesellschaft mit beschränkter Haftung*; in France *société à responsabilité limitée*; and in Poland *spółka z ograniczoną odpowiedzialnością*.

[16] S. Omlor, 'Digitalization…', op. cit., p. 4.

[17] Such requirements are present in the company law of particular Member States jurisdictions. For example: *Handelsgesetzbuch* in Germany; *Kodeks spółek handlowych* in Poland; and *Code De Commerce* in France.

[18] Article 22 of the Directive: 'A European central platform ("the platform") shall be established. The system of interconnection of registers shall be composed of: the registers of Member States; the platform; the portal serving as the European electronic access point. Member States shall ensure the interoperability of their registers within the system of interconnection of registers via the platform. Member States may establish optional access points to the system of interconnection of registers. They shall notify the Commission without undue delay of the establishment of such access points and of any significant changes to their operation.'

[19] The European Central Platform (ECP).

[20] Ibidem. BRIS functions as the European Access Point (EAP).

registers within the interconnection system through this platform. The interconnection of business registers (known as 'BRIS') operates by linking the business registers of all Member States. BRIS aims to enhance the transparency of EU company law by providing access to official and up-to-date information on companies across Member States.[21] However, there are instances of potential inconsistency between EU law and national legislation. In German law, for example, simplified online company registration may conflict with binding domestic company law, as it omits several obligations imposed on companies and notaries.[22]

At this point, it is also necessary to refer to notarial determination regarding beneficial ownership. Beneficial ownership is defined in Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ('4AMLD'), and in Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.[23] These instruments require Member States to ensure that corporate and other legal entities incorporated within their territories obtain and hold adequate, accurate, and up-to-date information concerning their beneficial ownership, including details of the beneficial interests held.[24] Such information must be registered and entered into central registers maintained by the Member States. These may be commercial, company, or public registers. Accordingly, Member State must provide unrestricted access to beneficial ownership information to competent authorities and financial intelligence units.[25] Certain obliged entities, such as banks or investment funds, are entitled to access to these registers within the framework of customer due diligence. Furthermore, and any person or organisation able to demonstrate a legitimate interest is also entitled to such access.[26]

---

[21] BRIS has been available since 8 June 2017 at https://e-justice.europa.eu/content_business_registers-104-en.do [accessed on 20 October 2025].

[22] Pursuant to Section 2(1) of the *Gesetz betreffend die Gesellschaften mit beschränkter Haftung* ('GmbHG'), the articles of association must be executed in notarial form and signed by all shareholders. Accordingly, pursuant to Section 10 of the *Beurkundungsgesetz* ('BeurkG'), the notary must establish the identity of the participants with certainty and resolve any doubts or ambiguities. Section 11 provides that the notary verifies the legal capacity of the participants, while Section 12 stipulates that the notary is responsible for verifying the authority to represent. Pursuant to Section 16, the notary is obliged to ensure that the contract is correctly understood by all parties with regard to the language in which the contract is drawn up. Finally, under Section 17, the notary reads the contract to the parties and ensures that the will of the parties is duly notarised. These provisions are related to the *Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten* ('GwG'), as notarial verification serves solely as a safeguard in cases of money laundering.

[23] Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, came into force on 15 June 2016 (hereinafter referred to as 'the 4AMLD').

[24] See Article 30 of the 4AMLD.

[25] See Article 30(3) of the 4AMLD.

[26] In relation to these actors, they shall additionally have access to the name, date of birth, nationality, residential address, and a statement of the nature and extent of the interest held by the beneficial owner, for example, 30% of the ordinary shares of the company.

A beneficial owner is defined as any natural person who ultimately owns or controls a corporate or other legal entity. Accordingly, in the Glossary to the Financial Action Task Force (FATF) Recommendations, the beneficial owner refers to the natural person or persons who ultimately own or control a customer, or the natural person on whose behalf a transaction is being conducted.[27] It also includes those persons who exercise ultimate effective control over a legal person or arrangement. However, references to 'ultimately owns or controls' and 'ultimate effective control' concern situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control.[28] A shareholding of 25% plus one share, or an ownership interest of more than 25% in the customer held by a natural person, is regarded as an indication of direct ownership. A shareholding of 25% plus one share, or an ownership interest of more than 25% in the customer held by a corporate entity under the control of a natural person or persons, or by multiple corporate entities under the control of the same natural person or persons, is regarded as an indication of indirect ownership. However, Member States retain the right to determine that a lower percentage may also indicate ownership or control.[29]

As illustrated by German law and the distinct prerogatives of notaries, their role in the process of ownership determination is instrumental. They provide legal advice regarding the documents required to establish a company (the articles of association, the application for registration with the commercial register, and the list of shareholders), as well as notarising and verifying the legal validity of the aforementioned documents. Notaries also verify proof that the required minimum share capital has been paid. Finally, they generate authentic electronic copies of all documents, seal them electronically, and securely transmit them, together with machine-readable data, to the commercial register. In Spain, similarly to Germany, the notary's role arises in the process of company formation. The information and documents prepared during this process are verified by the notary in accordance with the relevant provisions of national law. The notary issues a deed, which is subsequently registered in the Company Register and then within the EU system of interconnected registers. Once the deed has been registered, the company is officially established in accordance with both national and EU law.

Registers are obliged to make all pertinent information about companies available to the public. This includes details such as the company's legal form, registered seat, capital, and legal representatives. By disclosing this information, companies facilitate the identification of their legal representatives and other relevant data. Such identification is crucial for establishing and maintaining business relationships, as it enables the formation of obligations with and through the company. Individuals are entitled to access the information and documents available in BRIS. The Member States'

---

[27] The Financial Action Task Force (FATF) is an international policy-making and standard-setting body dedicated to combating money laundering and terrorist financing. It was established by the G7 in 1989 in response to growing concerns about money laundering.

[28] J. Hatchard, 'Money Laundering, Public Beneficial Ownership Registers and the British Overseas Territories: the impact of the Sanctions and Money Laundering Act 2018 (UK)', *Denning Law Journal*, 2018, Vol. 30, p. 188.

[29] See Article 3(6)(i) of the 4AMLD.

registers may also contain information on foreign branches and cross-border mergers of companies.[30] However, the Directive provisions relating to the interconnection of registers do not apply to branches opened in a Member State by a company that is not governed by the law of a Member State.[31] The Directive permits Member States to charge fees for access to information from the system of interconnected registers. Directive (EU) 2017/1132 does not impose any restrictions concerning the collection of fees for the use of information from this system. Therefore, Member States may impose such charges in accordance with their respective national laws. The system of interconnected registers should not present any technical barriers to the collection of such fees.[32] Importantly, the Commission is required to publish a report on the functioning of the system of interconnected registers.[33] It is essential that these reports include the technical and financial complexities inherent in the operation of this system.[34]

---

[30] See https://www.e-justice.europa.eu [accessed on 20 December 2018].

[31] Recital 25 of Directive 2017/1132: 'Cross-border access to business information on companies and their branches opened in other Member States can only be improved if all Member States engage in enabling electronic communication to take place between registers and transmitting information to individual users in a standardised way, by means of identical content and interoperable technologies, throughout the Union. This interoperability of registers should be ensured by the registers of Member States ("domestic registers") providing services, which should constitute interfaces with the European central platform ("the platform"). The platform should be a centralised set of information technology tools integrating services and should form a common interface. That interface should be used by all domestic registers. The platform should also provide services constituting an interface with the portal serving as the European electronic access point, and to the optional access points established by Member States. The platform should be conceived only as an instrument for the interconnection of registers and not as a distinct entity possessing legal personality. On the basis of unique identifiers, the platform should be capable of distributing information from each of the Member States' registers to the competent registers of other Member States in a standard message format (an electronic form of messages exchanged between information technology systems, such as, for example, xml) and in the relevant language version.'

[32] Pursuant to recital 37 of Directive 2017/1132, the Directive 'should not prejudge any specific technical solution as the payment modalities should be determined at the stage of adoption of the implementing acts, taking into account widely available online payment facilities'.

[33] Article 162 of Directive 2017/1132: '1. The Commission shall, not later than 8 June 2022, publish a report concerning the functioning of the system of interconnection of registers, in particular examining its technical operation and its financial aspects. 2. That report shall be accompanied, if appropriate, by proposals for amending provisions of this Directive relating to the system of interconnection of registers. 3. The Commission and the representatives of the Member States shall regularly convene to discuss matters covered by this Directive relating to the system of interconnection of registers in any appropriate forum. 4. By 30 June 2016, the Commission shall review the functioning of those provisions which concern the reporting and documentation requirements in the case of mergers and divisions and which have been amended or added by Directive 2009/109/EC of the European Parliament and of the Council, and in particular their effects on the reduction of administrative burdens on companies, in the light of experience acquired in their application, and shall present a report to the European Parliament and the Council, accompanied if necessary by proposals to amend those provisions.'

[34] Ibidem.

THE IMPLICATIONS OF THE CJEU JUDGMENT IN THE *MANNI* CASE

Company registers contain a vast amount of data protected under EU law, the inclusion of which in such registers has significant consequences. Hence, it is necessary to mention a landmark judgment concerning EU data protection law, arising from a factual background associated with what is now referred to as 'the right to be forgotten'.[35] Signore Salvatore Manni was the sole director of an Italian company, *Immobiliare e Finanziaria Salentina Srl*. He declared insolvency in 1992, and the company was removed from the Italian Companies Register in 2005. However, Signore Manni remained identifiable as the administrator of that company in the register. In December 2007, Mr Manni, as director of another company that had been awarded a contract to build a tourist complex in Italy, brought an action against the Lecce Chamber of Commerce. He alleged that the Chamber had acted in a manner detrimental to his new construction company, making it unable to continue its operations or enter into transactions. Furthermore, he sought the deletion of his personal data from the records relating to *Immobiliare e Finanziaria Salentina Srl*. The Court of Lecce upheld his claims and ordered the Lecce Chamber of Commerce to anonymise, though not to remove, the data concerning Signore Manni, and to pay him compensation for the damage suffered. The Italian Supreme Court, referring to the 'right to be forgotten' as a fundamental instrument for the protection of personal identity, requested a preliminary ruling from the Court of Justice of the European Union (CJEU). It asked CJEU whether the protection of personal data grants the data subject the right to obtain the deletion or anonymisation of their data published in the companies register after a certain period of time; whether the requirement that personal data be kept in a form permitting the identification of data subjects for no longer than is necessary for the purposes for which they were collected applies in such a context; and finally, whether

> 'Member States may, and indeed must, allow individuals (…) to request the authority responsible for maintaining the companies register to limit, after a certain period has elapsed from the dissolution of the company concerned and on the basis of a case-by-case assessment, access to personal data concerning them and entered in that register.'[36]

First of all, the judgment was delivered on the basis of the no longer valid[37] Directive 95/46/EC (Data Protection Directive), which was repealed by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as 'the GDPR'). Nevertheless, the judgment may be regarded as having a universal application, since, even in the light of the changes introduced by the GDPR, the substance of the CJEU's reasoning remains relevant.[38] This analysis, in fact, concerns the obligations

---

[35] *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*, Case C-398/15, judgment of the Court (Second Chamber), 9 March 2017; ECLI:EU:C:2017:197 (hereinafter referred to as 'the *Manni* case').

[36] Para. 30 of the CJEU judgment in the *Manni* case.

[37] From 24 May 2018, when the GDPR was implemented.

[38] Article 17 of Regulation (EU) 2016/679 of the European Parliament and of the Council

of public authorities responsible for maintaining company registers.[39] The data concerning Signore Manni recorded in the register fall within the category of personal data, since 'the fact that information was provided as part of a professional activity does not mean that it cannot be characterised as personal data.'[40] Moreover, the authority maintaining the register is a 'controller' that carries out the 'processing of personal data' by 'transcribing and keeping that information in the register and communicating it, where appropriate, on request to third parties'.[41] The CJEU judgment emphasised the obligation of disclosure, noting that it arises from the purpose of the provisions of Directive 95/46/EC.[42] In general, the objective of disclosing information in company registers is to protect, in particular, the interests of third parties in relation to joint-stock companies and limited liability companies, since the only safeguards such companies offer to third parties are their assets. Consequently, the key documents of the company concerned must be disclosed. This is necessary to enable third parties to become acquainted with their contents and with other relevant information concerning the company. This includes detailed information concerning the individuals authorised to make binding decisions on behalf of the company. Additionally, the CJEU ruled that Article 54(3)(g) of the EEC Treaty refers to the need to protect the interests of third parties generally,

---

of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR): '1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). 2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. 3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims.' See also recitals 65 and 66 of the GDPR.

39 Para. 31 of the CJEU judgment in the *Manni* case.

40 Ibidem, para. 34.

41 Ibidem, para. 35.

42 See ibidem, para. 49.

without distinguishing or excluding any categories falling within the scope of that term.[43] Consequently, the third parties referred to in that article cannot be limited solely to the creditors of the company concerned.[44] Hence, the CJEU judgment also established that the purpose of disclosure is 'to protect, in particular, the interests of third parties in relation to joint-stock companies and limited liability companies, since the only safeguards they offer to third parties are their assets', and 'to guarantee legal certainty in relation to dealings between companies and third parties in view of the intensification of trade between Member States'.[45]

In concluding the relevance of the *Manni* case, the CJEU explained that a person who seeks to restrict access to his or her personal data published in company registers has no right to request the deletion of such data, even after the company concerned has ceased to exist. Nonetheless, the individual retains the right to object to the processing of their data, a right that depends on the particular circumstances of the case and the existence of legitimate reasons. Finally, the CJEU underlined the importance of considering the purpose of data processing when assessing whether a data subject can obtain deletion or blocking of data. In this context, the Court ruled that, even though such data consist of information relating to professional activity, they still constitute personal data.

THE IDENTIFICATION OF THE NOTARY'S OBLIGATIONS AND ITS RELATION TO THE EIDAS REGULATION

Another example of the significant impact of digitalisation on European company law is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (hereinafter referred to as 'the eIDAS Regulation'), which repealed, as of 1 July 2016, the Electronic Signatures Directive 1999/93/EC[46] (hereinafter referred to as 'the eSignature Directive').[47]

---

[43] See ibidem, para. 51.

[44] See also judgment of the CJEU in Case C-97/96, *Verband Deutscher Daihatsu-Händler eV v. Daihatsu Deutschland GmbH*, ECLI:EU:C:1997:581; order of the CJEU in Cases C-435/02 and C-103/03, *Axel Springer AG v. Zeitungsverlag Niederrhein GmbH & Co. Essen KG*, ECLI:EU:C:2004:552; judgment of the CJEU in Case C-138/11, *Compass-Datenbanken GmbH v. Republik Österreich*, ECLI:EU:C:2012:449; judgment of the CJEU in Case C-615/13 P, *ClientEarth and PAN Europe v. EFSA*, ECLI:EU:C:2015:489; and judgment of the CJEU in Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner and Digital Rights Ireland Ltd*, ECLI:EU:C:2015:650. Each of the above-mentioned cases was decided at a different time; nevertheless, they all convey a single, concrete principle – the right to be forgotten – consistent with the protection of personal data through company registers and the temporal availability of such data.

[45] Based on the provisions of Directive 68/151. See also paras. 49 and 50 of the CJEU judgment in the *Manni* case.

[46] See recital 73 of the Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014) (hereinafter referred to as the 'eIDAS Regulation').

[47] See the eIDAS Regulation; Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing

The eIDAS Regulation governs electronic identification and trust services for electronic transactions within the internal market of the European Union. It ensures that various actors and businesses can use their national electronic identification schemes ('eIDs') to access public e-services in other EU Member States where such eIDs are recognised. It also establishes a European internal market for electronic signatures, electronic seals, time stamps, electronic delivery services, and website authentication. The eIDAS Regulation addresses two main issues. Firstly, citizens were previously able to use their eIDs only in the Member State of their habitual residence. This limitation created difficulties regarding cross-border trusted identification and online authentication required in everyday activities (e.g. cross-border healthcare).[48]

The Regulation addresses two main issues. The primary concern is that citizens are unable to use their electronic identification to verify their identity in another Member State if the national electronic identification schemes of the respective Member States are not recognised in others. This creates difficulties for all cross-border online services that require a higher level of trusted identification and authentication, such as cross-border healthcare or online public procurement. The second issue concerns the legal validity of trust services. These consist of the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services, and certificates related to these services, as well as the creation, verification and validation of certificates for website authentication or the preservation of electronic signatures, seals or certificates related to these services.[49] *A contrario*, the eSignature Directive was criticised for focusing solely on electronic signatures, while neglecting other trust services. For this reason, the eIDAS Regulation also applies to other forms of digital certification, such as electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, and certificate services for website authentication. This is a closed list; however, Member States are free to recognise at the national level other types of qualified trust services and to maintain or introduce national provisions relating to non-harmonised trust services.[50] Each type of trust service may be used in legal proceedings as evidence.[51] Unless otherwise provided by the eIDAS Regulation, Member States may determine the legal effect of trust services.[52] Pursuant to Article 22 of the eIDAS Regulation, Member States are required to establish, maintain and publish lists containing information on

---

the European Digital Identity Framework (OJ L, 2024/1183, 30.4.2024); and Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (OJ L 169, 30.6.2017).

48 See C. Cuijpers, J. Schroers, 'eIDAS as guideline for the development of a pan-European eID framework in FutureID', *Radboud Repository of the Radboud University, Nijmegen*, 2014; https://dl.gi.de/handle/20.500.12116/2636 [accessed on 29 December 2022], para. 3.2.

49 See Article 3(16) of the eIDAS Regulation. The cited wording of this Article reflects the text of the basic regulation as originally adopted. This provision was subsequently amended by Regulation (EU) 2024/1183, and the cited version is therefore no longer the wording currently in force.

50 Recitals 25 and 24 of the eIDAS Regulation.

51 See recital 22, and Articles 25, 35, 41, 43 and 46 of the eIDAS Regulation.

52 See recital 22 of the eIDAS Regulation.

qualified trust service providers. Trust service providers that meet the necessary criteria are designated as 'qualified' and are authorised to use the EU trust mark, which serves to indicate the provision of qualified trust services in a clear and easily identifiable manner.[53] Qualified trust service providers are supervised by an authority designated by each Member State.[54] A supervisory authority may be established within national territory and designated by the respective Member State; however, upon mutual agreement, another authority established in a different Member State may be designated to supervise qualified trust service providers in the designating Member State.[55] The principal role of the supervisory authority is to ensure, through *ex ante* and *ex post* supervisory reviews, that qualified trust service providers and the qualified trust services they offer meet the requirements set out in the Regulation, and to supervise non-qualified trust service providers established within the territory of the designating Member State.[56]

Both individuals and companies may use their own electronic identification systems. This enables access to electronic services across EU countries where electronic identity confirmation is required. Liability for failure to comply with the relevant obligations, such as notifying the Member State, rests with the entity issuing the electronic identification measures and processing the authentication.[57] The general rules of liability apply to the eIDAS Regulation, and it therefore does not affect the definitions of compensation or applicable procedural norms, including national rules on the burden of proof.

The impact of the eIDAS Regulation on the work of notaries is straightforward and concerns the confirmation of the identity of the person submitting the signature, which must be verified with the notary's seal.[58] According to the eIDAS Regulation, an electronic signature must be accompanied by a qualified certificate.[59] The qualified certificate must meet the following requirements:[60]

- indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;
- a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates, including at least the Member State in which that provider is established and, for a legal person, the name and, where applicable, registration number as stated in the official records; for a natural person, the person's name;
- at least the name of the signatory or a pseudonym;

---

53 Article 23 of the eIDAS Regulation.
54 Article 17 of the eIDAS Regulation.
55 Ibidem.
56 Article 17(3) of the eIDAS Regulation.
57 Article 13 and recital 18 of the eIDAS Regulation.
58 See Article 28 of the eIDAS Regulation.
59 The entity that subscribes to or owns a certificate is identified as the Certification Authority (CA), and the document containing the necessary data relating to the certificate is known as the Certification Practice Statement (CPS). However, the substance of certification is closely related to IT matters.
60 See Annex I to the eIDAS Regulation.

- electronic signature validation data that corresponds to the electronic signature creation data;
- details of the beginning and end of the certificate's period of validity;
- a certificate identity code, which must be unique for the qualified trust service provider;
- an advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
- the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in the foregoing requirement is available free of charge;
- the location of the services that can be used to verify the validity status of the qualified certificate;
- appropriate indication of a qualified electronic signature creation device.

In the legislation of several Member States, the issuance of certificates by notaries, authentication of signatures, and verification of copies with original documents, extracts or duplicates may be formalised through the use of a qualified electronic signature, provided that the specific form of certification requires such authentication. The validity of a notarial electronic document or its certification is equivalent to that of a notarial deed.

Electronic signatures are issued through qualified devices.[61] These qualified devices must comply with the following requirements:[62]

- they must ensure, by appropriate technical and procedural means, that at least the confidentiality of the electronic signature creation data used for signature creation is reasonably secured; that the electronic signature creation data used for signature creation can occur only once; that such data cannot, with reasonable assurance, be derived; and that the electronic signature is reliably protected against forgery using currently available technology. The electronic signature creation data used for signature creation must be reliably protected by the legitimate signatory against use by others;
- they must not alter the data to be signed or prevent such data from being presented to the signatory prior to signing;
- the generation or management of electronic signature creation data on behalf of the signatory may be carried out exclusively by a qualified trust service provider;
- qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate such data only for back-up purposes, provided specific requirements are met.[63]

The qualified device must have a certificate issued by the relevant public or private entities designated by the Member States, confirming compliance with the requirements of Annex II to the Regulation. Certification must involve a security

---

[61] See Article 30 of the eIDAS Regulation.

[62] See Annex II to the eIDAS Regulation

[63] Ibidem: the security of the duplicated datasets must be equivalent to that of the original datasets, and the number of duplicated datasets shall not exceed the minimum necessary to ensure continuity of the service.

assessment procedure carried out in accordance with one of the recognised standards for the security assessment of IT products.[64] Alternatively, the devices may comply with other procedures that ensure comparable levels of safety and are applied by the designated public or private entity.[65] Without undue delay, pursuant to Article 31 of the eIDAS Regulation,[66] the Commission shall prepare, publish, and maintain a list of certified qualified devices for electronic signature. Within one month of the completion of certification, Member States must provide the Commission with information concerning qualified devices.

Apart from electronic signatures, seals have also been transformed into their digital form. The eIDAS Regulation recognises two types of electronic seal: the basic electronic seal and the advanced electronic seal. Pursuant to Article 3(25) of the eIDAS Regulation, an electronic seal consists solely of data in electronic form, attached to or logically associated with other data in electronic form to ensure the originality and integrity of the document. The advanced electronic seal is uniquely linked to its creator and allows for their identification. The creator of the advanced electronic seal can, with a high level of confidence, use the electronic seal and the data to which it relates in such a way that any subsequent alteration of the data is detectable.[67]

The electronic seal may replace the notarial seal. However, the legal effects of the use of an electronic seal are limited to certain legal proceedings only, as it does not meet the requirements of a qualified electronic seal. It enjoys the presumption of the integrity of the data and the correctness of the origin of that data to which the qualified electronic seal is linked. Furthermore, a qualified electronic seal based on a qualified certificate issued in one Member State is recognised as a qualified electronic seal in all other Member States.[68]

CONCLUSION

Digitalisation is an unavoidable phenomenon. Sooner or later, most daily activities will be transformed into digital form. This process will undoubtedly streamline many procedures as a result of the legal provisions described in this article. BRIS undoubtedly constitutes a set of useful solutions; however, as can be observed from the German example, it remains imperfect and is not equally adapted to the specificities of each Member State. Moreover, in the context of GDPR, data protection in registers does not fully ensure the effectiveness of the 'right to be forgotten', since personal data stored in registers cannot be permanently deleted. A step in the right direction is certainly the adoption of the eIDAS Regulation, which contains provisions covering a wide range of trust services. This stands in contrast to the eSignature Directive, which related solely to electronic signatures and was therefore insufficient, given the multitude of other types of trust services now available. As a consequence of digitalisation, the nature of

64 See Article 30 of the eIDAS Regulation.
65 See Article 30(1) of the eIDAS Regulation.
66 See Article 31 of the eIDAS Regulation.
67 See Article 36 of the eIDAS Regulation.
68 See Article 35 of the eIDAS Regulation.

notarial work is changing rapidly. This is due to the fact that the physical presence of a notary may no longer be necessary when incorporating a company. Nonetheless, in some Member States, the notary's presence remains obligatory for certain acts, such as the notarisation of wills, verifying a person's identity, or confirming the legal capacity of documents required for company incorporation. Furthermore, with regard to beneficial ownership, and pursuant to 5AMLD, the work of legal practitioners, including notaries, serves as an additional and important layer in the prevention of money laundering. It is certain that further regulations will follow in the near future in response to the continuing development of digital technologies.

BIBLIOGRAPHY

Bregeš Ž., Jakupak T., 'Digitalization of business register', *InterEULawEast*, 2017, Vol. IV, Issue 2.

Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni, Case C-398/15, judgment of the Court (Second Chamber), 9 March 2017; ECLI:EU:C:2017:197.

Cuijpers C., Schroers J., 'eIDAS as guideline for the development of a pan-European eID framework in FutureID', *Radboud Repository of the Radboud University, Nijmegen*, 2014; https://dl.gi.de/handle/20.500.12116/2636 [accessed on 29 December 2022].

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Single Market Strategy for Europe*, COM(2015) 192 final.

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Commission Work Programme 2017. Delivering a Europe that protects, empowers and defends*, COM(2016) 710 final.

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – EU eGovernment Action Plan 2016–2020*, COM(2016) 179 final.

European Parliament, *Resolution of 16 May 2017 on the EU eGovernment Action Plan 2016–2020 (2016/2273(INI))*, OJ C 307, 30.8.2018.

Hatchard J., 'Money Laundering, Public Beneficial Ownership Registers and the British Overseas Territories: the impact of the Sanctions and Money Laundering Act 2018 (UK)', *Denning Law Journal*, 2018, Vol. 30.

Llopis Benlloch J.C., 'Notaries and digitalisation of company law', *ERA Forum*, 2018, Vol. 19.

Omlor S., 'Digitalization and EU Company Law, Innovation and Tradition in Tandem', *European Company Law*, 2018.

Wachter T., 'Neues zum Europäischen Gesellschaftsrecht: Digitalisierung im GmbH-Recht (I)', *GmbH-StB*, 2018, No. 7.

Cytuj jako:

Braun T. (2025), *Digital processes in EU company regulations and their implications for registry practices*, Ius Novum (Vol. 19) 4, 175–189. DOI 10.2478/in-2025-0043