ADITUM
Enrich your Research

International Journal of Business Research and Management

Research Article

The Evolving Legal Framework for Data Protection: Comparing the Protective Measures for Personal Data and Trade Secrets

Željka Krolo Ivanov[1], Ana Rački Marinković[2*]

[1] Mag. iur., Spec. Int. Prop., Lawyer.

[2] Associate Professor, PhD, Veleučilište studija sigurnosti, Veslačka 2A, Zagreb, Croatia.

Article Information

Received: October 20, 2026
Accepted: October 30, 2026
Published: November 04, 2026

***Corresponding Author:** Ana Rački Marinković, Associate Professor, PhD, Veleučilište studija sigurnosti, Veslačka 2A, Zagreb, Croatia.

Citation: Željka K Ivanov, Ana R Marinković., (2026). "The Evolving Legal Framework for Data Protection: Comparing the Protective Measures for Personal Data and Trade Secrets". International Journal of Business Research and Management 5(3); DOI: 10.61148/3065-6753/IJBRM/111.

Copyright: © 2026. Ana Rački Marinković. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract:

Businesses today collect, generate, and use various types of data, including both personal and non-personal (business) data. The European Union has established regulatory frameworks addressing the protection of certain data types. Personal data is governed by the General Data Protection Regulation, which mandates the implementation of organisational, technical, and security measures. Business data, qualifying as trade secrets, is protected under the Trade Secret Directive, contingent upon the provision of reasonable measures to preserve secrecy to be afforded protection. Given the inherent vulnerability of both personal data and trade secrets, this paper aims to provide a systematic comparative analysis of the protective measures required for personal data and trade secrets, finding similarities and identifying synergies and 'best practice' overlaps. Although the required level of protective measures depends on the circumstances of the case, there is potential for common approaches. The adoption of data mapping and best practices is recommended to reduce the risk of exposure or unauthorised access to both trade secrets and personal data.

Keywords: personal data, trade secrets, General Data Protection Regulation, Trade Secrets Directive, protective measures, reasonable measures

1. INTRODUCTION

In the digital economy, businesses collect, generate, and use vast amounts of data, which can be understood under a common concept of business data. Yet no legal, generally accepted definition of business data exists in the European Union (EU). Under the common concept of business data, many types of data can be differentiated, from raw data, which may not be of great value to business, to more processed, aggregated, and structured data, which becomes very valuable, in particular in cases where such data is given a meaning.[1] Scholars have distinguished such data in the semantic sense from pure synthetic data when discussing whether data can be protected by trade secrets.[2][3] When decomposed to the level of individual data, such data may also consist of personal data. With the growing importance of data in the data economy, the EU has regulated protection issues with respect to different types of data and addressed such data sharing and re-use in several horizontal and industry-specific pieces of legislation.[4]

When it comes to personal data, for most European data regulators, entrepreneurs, and governmental bodies, the General Data Protection Regulation[5] (GDPR) is probably the first association.[6] Under GDPR, personal data is defined as information relating to an identified or identifiable natural person[7][8], which definition covers a wide cluster of personal information (both objective, such as a name and surname, and subjective, such as comments on social media, as long as the data subject could be identified by them[9]). Therefore, personal data[10] may reveal sensitive information and serve as a target for unauthorised usage.

A similar position holds trade secrets, protected under the Trade Secrets Directive[11]. Directive identifies trade secrets as a vulnerable category of data, stating that innovative businesses "are increasingly exposed to dishonest practices aimed at misappropriating trade secrets, such as theft, unauthorised copying, economic espionage or the breach of confidentiality requirements, whether from within or from outside of the Union."[12]

A significant regulatory asymmetry exists due to the fragmented approach toward protecting

---

[1] Tanya Aplin, Alfred Radauer, Martin A Bader, Nicola Searle, 'The Role of EU Trade Secrets Law in the Dana Economy: An Empirical Analysis' (2023) 54 (6) International Review of Intellectual Property and Competition Law 841

[2] Ulla-Maija Mylly, 'Trade Secrets and the Data Act' (2024) 55 (3) International Review of Intellectual Property and Competition Law 373

[3] The Organization for Economic Cooperation and Development (OECD) categorizes data as follows: corporate data; end-customer data (business-to-consumer; B2C); human resources data; merchant data (business-to-business; B2B); and technical data according to David Nguyen, Marta Paczos, 'Measuring the economic value of data and cross-border data flows: A business perspective' (2020) 297 OECD Digital Economy Papers <https://doi.org/10.1787/6345995e-en> accessed 27 March 2026

[4] Aplin (n 1) 827-828

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) [2016] OJ L 119/1

[6] As a regulation, GDPR is a general and most comprehensive European data protection framework, directly binding for all members of the European Union and indirectly binding for data processors established outside of the European Union.

[7] GDPR, art. 7

[8] In accordance with article 4 of the GDPR an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[9] Hypothetically, probably having a record about someone's religious beliefs without any other information wouldn't be considered as personal data. In other words, information *per se* or a combination of two or more information regarded as personal data only if data subject by such data could be identified.

[10] The list thereby is not exhausted.

[11] Directive (EU) 2016/943 of the European parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Trade Secrets Directive) [2016] OJ L 157/1

[12] Trade Secrets Directive, recital 4

Copyright © Ana Rački Marinković

personal data and trade secrets within the same corporation. This creates an operational divergence where the GDPR and the Trade Secrets Directive are treated as unrelated obligations, despite their shared reliance on similar security infrastructures. Although both data categories are highly vulnerable to unauthorised access, they are frequently managed through independent, non-communicating frameworks, overlooking the substantive legal and technical overlaps between the GDPR and the Trade Secrets Directive.

A significant number of discussions in academic literature are dedicated to the intersection between different types of data with respect to the protection afforded, in particular, between trade secrets law and data privacy law.[13] However, discussions are focused mainly on finding similarities and differences between legal regimes. A number of authors have investigated the relations between personal data and trade secrets, specifically in situations where personal data is part of the semantic data that is protected by trade secrets. Discussions around the prevalence of these rights are to be mentioned[14], mostly considering Article 15 (1) h of the GDPR, providing the right of access, which may be balanced with the rights and freedoms of others, including intellectual property and trade secrets.

This paper focuses on the extent to which technical, legal, and organisational measures set forth under GDPR and the Trade Secrets Directive may be integrated into a single, proactive information governance strategy. This research examines the potential for harmony between these two frameworks, particularly since both rely on security postulates while originating from different legal foundations. Furthermore, this paper investigates the divergent legal consequences that arise when a company fails to implement adequate protective measures under each regime. It explores the asymmetry of risk between the threat of administrative fines under the GDPR compared to the risk of a permanent loss of intellectual property under trade secret law, which serve as motivators for corporate compliance. Ultimately, the study seeks to determine if a unified 'data mapping' approach provides a superior defence against unauthorized access when personal data and commercially valuable trade secrets overlap within the same dataset.

This paper aims to provide a systematic comparative analysis of the protective measures required for personal data and trade secrets to identify synergies and 'best practice' overlaps. We argue that while the GDPR and Trade Secrets Directive obligations arise from distinct legal bases, these frameworks require organisations to utilise the best available technical and organisational measures at the time, rather than specific named tools. Insofar as their implementation is concerned, they both rely on nearly identical 'state-of-the-art' technical and organisational measures. Therefore, a holistic approach is not only more efficient but legally necessary when personal data constitutes a trade secret.

This research employs a systematic doctrinal examination of EU legislative frameworks, specifically the GDPR and the Trade Secrets Directive, alongside a review of emerging jurisprudence and literature review to determine the standard of 'reasonableness' and 'appropriateness' in data protection.

Building on this methodological framework, the subsequent sections are organised to facilitate a direct comparison of these two regimes. After the introduction, the paper is followed by the first part of this paper, which analyses GDPR. The second part gives an overview of the Trade Secrets Directive. In the third part, the authors compare technical, organisational, and security measures imposed by the GDPR and the Trade Secrets Directive, finding similarities and possible common usage together with an overview of the interrelationship between them. In conclusion, the main points are summarised, and recommendations for further research are given.

2. OVERVIEW OF THE GENERAL DATA PROTECTION REGULATION - HOW TO PROTECT PERSONAL DATA?

GDPR should be implemented as a mandatory regulatory framework in each business or non-

[13] Sharon K. Sandeen, 'Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law' (2006) 6 Michigan State Law Review 667-707; Pamela Samuelson, 'Privacy as Intellectual Property?' (2000) 52 (5) Stanford Law Review 1-42; Lital Helman, 'Trade Secrets and Personal Secrets' University of Richmond Law Review (2021) 55 (2) 447-489

[14] Bart Custers, Anne-Sophie Heijne, 'The right of access in automated decision-making: The scope of Article 15(1)h GDPR in theory and practice' (2022) 46 Computer Law & Security Review 1-17; Gianclaudio Malgieri, 'Trade Secrets v Personal Data: A Possible Solution for Balancing Rights' (2016) 6 (2) International Data Privacy Law 102–116

Copyright © Ana Rački Marinković

business subject. The GDPR is divided into eleven chapters, covering general provisions – Chapter 1 (Articles 1 to 4), Chapter 2- Principles (Articles 5 to 11), Chapter 3-Rights of the Data subjects (Articles 12 to 23), Chapter 4- provisions related to the Data controllers and Data processors (Articles 24 to 43). Chapter 5- Transfers of personal data to third countries or international organisations (Articles 44 to 50), Chapter 6-Independent Supervisory (Articles 51 to 59), Chapter 7-Cooperation and Consistency (Articles 60 to 76), Chapter 8-Remedies, liability and penalties (Articles 77 to 84), Chapter 9- Provisions relating to specific processing situations (Articles 85 to 91), Chapter 10- Delegated acts and implementing acts (Articles 92 to 93), Chapter 11- Final provisions (Articles 94 to 99). Requirements outlined in Article 32 of the GDPR are part of Chapter 4 and explained in the next part of the paper.

2.1. RECOMMENDED DATA PROTECTION ORGANISATIONAL, TECHNICAL AND SECURITY MEASURES

Organisational, technical, and security measures are not defined in detail under GDPR. They must be implemented in the data controller's assessment[15]. A decision should be made in light of several factors, including available technologies, implementation costs, and the nature, scope, and purpose of data processing. Furthermore, the likelihood and severity of potential risks to individuals' rights must be a key consideration.[16] According to the European Data Protection Board (EDPB), organisations' measures often target employees by providing educational courses focused on raising awareness[17], or adopting internal privacy policies, confidentiality agreements, or signing confidentiality statements integrated into an employment agreement or as a document *per se*. The data controller must be aware of who within the organisation processes personal data. Therefore, employees are subject to the 'know your role' rule, under which data categories and employees authorised for processing such data are identified.[18][19] Sufficient technical and security measures were debated before the competent supervisory data protection authorities. Dutch Data Protection Authority (Autoriteit Persoonsgegevens), in a decision related to Stichting Hogeschool van Arnhem en Nijmegen, dated 15 December 2025[20], ruled on the breach of Article 32 of the GDPR due to a lack of organisational, technical, and security measures. During the investigation the competent authority identified key failures that led to the penalization of the data controller: Insufficient measures against SQL injection, excessive database access rights, poor password policy, and a lack of adequate processes to execute the retention policy. Sweden's competent authority (Swedish Authority for Privacy Protection, IMY) found similar conclusions related to the breach of Article 32 of the GDPR in the decision Sportadmin i Skandinavien AB, dated 26 January 2026.[21] The data controller did not have sufficient measures against SQL injection in place. The competent authority identified further failures referring to obligations set forth under Article 32 of the GDPR: lack of a restrictive system privileges; the non-subjective, mandatory, with automated security checks, code review process,

[15] Sanjay Sharma *Data Privacy and GDPR Handbook* (John Wiley & Sons 2020) 11, 30-31

[16] *Ibid. 3*

[17] "It is essential to make employees or users handling personal data (data handlers) aware of the risks related to privacy, inform them of the measures taken to address the risks and the potential consequences in case of failure" European Data Protection Board (EDPB) <https://www.edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en> accessed 27 March 2026

[18] Art. 28 GDPR proscribes where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

[19] It is important to state that the same subject might be data processor, data controller, joint controller, third-party, depending on the nature and purposes of the data processing.

[20] Case 2024-024797 *Autoriteit Persoonsgegevens v. HAN University of Applied Sciences* [2025], <https://autoriteitpersoonsgegevens.nl/system/files?file=2025-12/Boete%20HAN.pdf > accessed 27 March 2026

[21] Case IMY-2025-7801 *The Swedish Authority for Privacy Protection (IMY) v. Sportadmin i Skandinavien AB* [2026] <https://www.imy.se/globalassets/dokument/tillsynsskrivelser/2026/beslut-efter-tillsyn-enligt-gdpr_sportadmin-i-skandinavien-ab.pdf> accessed 27 March 2026

Copyright © Ana Rački Marinković

monitoring system with detection of attacks in real time. From the abovementioned decisions, it can be inferred that technical and security measures include, for example, measures against SQL injections, live-monitoring, and strong access control. To be reasonable, obviously, measures must correspond to the privacy risk. Also, a privacy policy in place without an enforcement procedure is not enough, states a competent Swedish authority. From the current state of case-law, only if procedures in force are executed then those measures may be considered as adequate under the GDPR.

According to the official working material of EDPB the following measures for reducing data privacy risks or data breaches, are indicated as acceptable: training employees on data protection, using up-to-date anti-virus and anti-malware, keeping systems up to date, implementing and revising access control policies, multi-factor authentication for sensitive data access, monitoring unusual data flows, enforcing disk encryption, making and testing backups regularly, and setting computers to auto-lock after inactivity"[22].

Generally, it should be concluded that implementation of measures must be adequate, and adequacy is to be tested before implementation, and during the personal data lifecycle. Such a conclusion is supported by the judgement of the Court of Justice of the European Union (CJEU), in case C-340/2021, which is highly relevant for the interpretation of Article 32 of the GDPR. The Court, *inter alia*, was questioned as to what the subject matter and scope of the judicial review of legality in the examination should be, as to whether the technical and organisational measures implemented by the controller are appropriate pursuant to Article 32 of the GDPR?[23] Referring to the cited question the Court stated that the assessment of the sufficient level of the technical, organisational, and security measures shall be performed in two stages. The first step is an assessment of the privacy risks and related consequences on the rights and freedoms of the data subjects. The second step should evaluate whether the measures implemented by the controller are appropriate to those risks. The Court highlighted that national courts must examine measures, considering the following: criteria referred to in Article 32 of the GDPR, circumstances of the case, and the related evidence available to the court. Therefore, the implementation of measures should follow an approach similar to the obligation outlined in Article 35[24] of the GDPR, related to high-risk processing activities.

3. OVERVIEW OF THE TRADE-SECRETS DIRECTIVE - HOW TO PROTECT TRADE SECRETS?

Information, whether know-how, business, or technological information, may help companies to achieve an advantage over their competitors and therefore, when kept secret, possesses a specific market (commercial) value. There may be other types of confidential business information that business entities keep secret for specific business reasons that do not necessarily have an economic value *per se*[25]. More complex (nontrivial) information that has commercial value is generally called trade-secrets and recognised as a form of intellectual property, as opposed to the broader notion that also encompasses other forms of confidential business information, usually referred to as business secrets.

Information that may qualify as trade-secrets includes a varied spectrum of data including a diversified range of strategic commercial information, such as information on customers and suppliers, business plans, etc. Specific personal data as such has neither commercial value nor is used by businesses to gain an

[22] <https://www.edpb.europa.eu/system/files/2025-03/edpb_summary_092022-012021_data_breach_en.pdf> accessed 27 March 2026

[23] Case C-340/21 *VB v Natsionalna agentsia za prihodite* [2023] ECR ECLI:EU:C:2023:986

[24] Art. 35 GDPR states "that where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks".

[25] Commission Staff Working Document: Impact assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, SWD [2013] 471, 113 <https:// eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013SC0471> accessed 27 March 2026

Copyright © Ana Rački Marinković

advantage on the market. However, a list of buyers or clients may supply a specific advantage on the market and is therefore qualified as a trade secret.

It is not possible to define a trade secret by listing all the information that can be used as such. Its definition is thus given by stating the essential elements that such information must satisfy for it to qualify as a trade secret. To qualify as a form of intellectual property, a trade secret must not be disclosed in public, and it must have commercial value because it is a secret, with appropriate steps undertaken to ensure its secrecy. This definition has been recognised internationally and is included in the Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS Agreement).[26] Since the TRIPS Agreement is mandatory for all members of the World Trade Organization, including the European Union, the Trade Secrets Directive follows this definition in Article 2, where it prescribes three requirements that need to be satisfied for certain information to be considered a trade secret in the European Union. First, information must be secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question. Information need not be absolutely secret, which would presuppose that it is known only to its holder, because the information that cannot be used would have no value; therefore, relative or substantial secrecy is all that is required.[27] However, it may be known to a particular circle of persons, which has to be limited (although it is not possible to set an upper boundary as to the acceptable number of people within the circle), but it should not be in the public domain. Nevertheless, all persons who know this information must, in a way, be obliged to keep it secret. As stated, this need not necessarily involve only information that is secret in its entirety. Information on which parts are not secret, but the fact that the way the information has been assembled is not known to the public, also fulfils the secrecy requirement.

The second condition is that information has commercial value precisely because it is secret (Article 2 of the Trade Secrets Directive). The commercial value means the holder has an interest in keeping that information secret, which is commercial and objective[28], whether actual or potential (Recital 14 of the Trade Secrets Directive)[29]. The third element of the definition is that "it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret," which will further be elaborated below.

The goal of the Trade Secrets Directive was to harmonise the legal protection of trade secrets at the EU level "so as to ensure that there is a sufficient and consistent level of civil redress in the internal market in the event of unlawful acquisition, use or disclosure of a trade secret" (Recital 10 of the Trade Secrets Directive). The scope of trade secret protection is harmonised by homogeneously identifying the circumstances in which legal protection of trade secrets is justified (Article 3 of the Trade Secrets Directive) and establishing conduct and practices which are to be regarded as unlawful acquisition, use or disclosure of a trade secret (Article 4 of the Trade Secrets Directive). The independent discovery or creation of the same information remains possible, and reverse engineering is considered lawful. This is because the Directive does not create any exclusive right to information protected as a trade secret. Thus, third parties are not prohibited from obtaining information by any practice which is, under the circumstances, in conformity with honest commercial practices. Before the Trade Secrets Directive was adopted, many Member States did not have rules aimed at safeguarding trade secrets during litigation, thus deterring victims of trade secret misappropriation from seeking redress in court.[30]

---

[26] The Agreement on Trade-Related Aspects of Intellectual Property Rights is Annex 1C of the Marrakesh Agreement Establishing the World Trade Organisation (WTO) signed on 15 April 1994 as a result of the 1986-94 Uruguay Round negotiations.

[27] Sharon K Sandeen, 'The limits of trade secret law: Article 39 of the TRIPS Agreement and the Uniform Trade Secret Act on which it is based' in Rochelle C Dreyfuss, Pauline Newman, Katherine J Strandburg (eds) *The law and theory of trade secrecy: a handbook of contemporary research* (Cheltenham 2012) 555

[28] It is up to case law to ensure that commercial value is established based on the objective interest of the need for keeping secrecy.

[29] In most cases, trade secrets are not in commerce and therefore can only have potential value.

[30] Commission Staff Working Document, (n 25) 216 outlines the problem of trade secret leakage in legal proceedings. The lack of effective measures for trade secret protection during court proceedings, with the consequent risk of losing

Copyright © Ana Rački Marinković

The provision on the preservation of confidentiality of trade secrets in the course of a legal proceeding (Article 9) is therefore considered one of the key provisions introduced by the Trade Secrets Directive. The contribution of the Directive in stipulating measures, procedures, and legal instruments in the case of trade secret infringement is indisputable.

3.1. REASONABLE MEASURES FOR PRESERVING SECRECY

Providing reasonable measures to preserve secrecy is an element of the definition of a trade secret. It may seem contradictory at first sight: what is the need for the legal protection of trade secrets at all, when measures for preserving secrecy have already been undertaken? The justifiability of this requirement is therefore often questioned, even more so since such a 'self-help' requirement is highly unusual in intellectual property law otherwise.[31]

Some authors understand that this requirement follows from the fact that trade secrets are not absolute rights: the law can only protect secrets that are also protected by their holder,[32] who thus proclaims to third parties that these data are protected. According to some, the explanation is literally hidden in the obligation of undertaking 'reasonable' measures for preserving secrecy: it replaces the obligation of undertaking measures for the full protection of secrecy. Legal protection comes into place after the holder has undertaken reasonable measures to keep information secret, so the holder does not have to introduce strict physical limitations and set up full isolation to render access to that information impossible. Both explanations seem valid.

Since the Trade Secrets Directive had to be incorporated into national Member States law by 9 June 2018, there was already a significant period in which harmonised trade secrets litigation exists, and trends emerging from the jurisprudence of Member States can be identified. The qualitative analysis of the key cases reported during the study undertaken by EUIPO reveals how the courts in the European Union have interpreted *inter alia* the definition of trade secrets, including reasonable steps as one of the elements of the definition. According to the study, one of the most common defences in litigation proceedings is that the claimant failed to take reasonable steps to protect the information[33]. Drawing a conclusion from the trends recognised, trade secret holders should put in place a trade secret protection management system, an important aspect of which is the identification of the company's trade secrets. Put simply, the holder must, first of all, know exactly what secret information has commercial value for him. Then, he must establish measures to protect such information from being disclosed. 'Precise identification of the object of protection' is not an explicit requirement for protection under Article 2 of the Trade Secrets Directive; it seems to emerge as a jurisprudential component of the 'reasonable steps' requirement in certain contexts[34].

---

control over trade secrets, makes recourse to legal actions often unappealing for trade secrets owners.

[31] A copyright owner can sue for infringement without first encrypting a website that displays his/her work or insisting that a concert hall search the audience for hidden recorders. In fact, protection does not require, as a condition, a copyright notice. Robert G Bone, 'Trade secrecy, innovation, and the requirement of reasonable secrecy precautions' in Dreyfuss (n 38) 47

[32] Mira Burri, Ingo Meitinger, 'The Protection of Undisclosed Information: Commentary of Article 39 TRIPS' in Thomas Cottier, Pierre Véron (eds) *Concise International and European IP Law: TRIPS, Paris Convention, European Enforcement and Transfer of Technology* (Kluwer Law International 2014) 3. Authors state that only under the condition that third parties pass a certain hurdle, thus proving their dishonest intentions to use the information, can the holder defend his trade secret by legal means.

[33] European Union Intellectual Property Office 'Trade secrets litigation trends in the EU' (2023) 64 <https://www.euipo.europa.eu/en/publications/trade-secrets-litigation-trends-in-the-eu> accessed 27 March 2026

[34] *Ibid.* 67 The Estonian Supreme Court ruled that, since the employer did not specify exactly what information qualified as a trade secret, but rather declared all company information confidential, the former employees were not liable for unlawful trade secret disclosure. Furthermore, the Düsseldorf Labour Court found that '[an] agreement which simply declares all matters and processes which become known in the course of the activity to be subject to secrecy and which also expressly refers to such processes which are not business secrets is insufficient.' Similarly, the Hungarian Supreme Court denied trade secret protection to information that was described only in an abstract and general manner in a subcontractor agreement. The Italian Supreme Court has also confirmed that, for a

Copyright © Ana Rački Marinković

The Trade Secrets Directive does not stipulate what reasonable measures should consist of, since it depends on the circumstances of the case, and it is impossible to define in advance. The Court of Appeal in Turin stated that measures shall be seen as reasonable if they do not make it easy for specialists in the sector to find out trade secrets using reverse engineering.[35] EUIPO study mentions a decision from the Düsseldorf Regional Court that stressed appropriate measures do not require 'optimal protection' or 'extreme security'. The court further elaborated various factors that must be taken into account in assessing the appropriateness of protection measures, namely: 1. the type of trade secret, 2. the specific circumstances of use, 3. the value of the trade secret and its development costs, 4. the nature of the information, 5. the importance for the company, 6. the size of the company, 7. the usual confidentiality measures in the company, 8. the type of labelling of the information, and 9. agreed contractual provisions with employees and business partners[36]. The particularities of the industrial sector in which the trade secret appears, including the risk of the unauthorised acquisition of the trade secret in that sector, could also be added to that list. Since the value of the trade secret itself has to be taken into account, it seems that the higher the value of the secret, the more sophisticated, costly, and comprehensive the expected protection by its holder.[37] Different courts, even in the same jurisdiction, have made different determinations on whether a policy of access restrictions through usernames and passwords is sufficient to meet the standards of reasonable steps, clearly suggesting that the analysis needs to be performed on a circumstance-specific basis[38]. However, this should be measured according to an objective criterion. Thus, it is not sufficient for the holder to undertake only those measures which he subjectively thinks ensure secrecy, and which are, objectively, not sufficient.[39] Measures can be judged to be reasonable and sufficient, even when there was a security breach, since the obligation to take reasonable protective measures is not an obligation of result to guarantee security[40].

What is apparent is that reasonable steps may be divided into three main categories: physical control measures, organizational measures (which should also include raising employee awareness), and legal measures assuring the commitment of employees and business partners to protect trade secrets.

Physical control measures, as a rule, ensure that confidential information does not fall into the hands of third parties. These are usually technical measures that aim to prevent third parties from getting to the content of secret information. Measures consisting of restricting access to information to a smaller circle of employees (on a need-to-know basis), or special restrictions of entry into areas where trade secrets are used, ensuring access to electronic files with a password or by encryption, could also be appropriate. In a case from Italy, the Court introduced a distinction between physical and cybersecurity measures for confidential information and engaged in a detailed assessment of the various measures put in place by the company to ensure that its information was kept secret[41]. Because the notion of 'reasonable steps' is a flexible concept, the

measure to be considered appropriate, it is implied that persons who have access to the information assumed to be confidential must be made aware of the holder's intention to keep it secret.

[35] Michaël De Vroey, Margo Allaerts, 'Trade secrets protection: an interim update of Belgian and EU case law,' (2021) 16 (12) Journal of Intellectual Property Law & Practice 1394

[36] European Union Intellectual Property Office (n 33) 65

[37] Burri (n 32) 3

[38] European Union Intellectual Property Office (n 33) 64

[39] *Ibidem.*

[40] De Vroey (n 35) 1394.

[41] European Union Intellectual Property Office (n 33) 141. Physical security had been guaranteed by a lock on the access door of the data centre and a volumetric alarm. Cybersecurity was guaranteed by several measures, including software restrictions on access to the company domain, a proprietary firewall system, a next-generation firewall (NGFW) appropriate to the nature and dimension of the company, a credential system for accessing corporate computers with a fragmentation of information based on duties of each employee, specific authorisations for accessing certain corporate data, and the requirement of complex passwords with a minimum of eight characters. All these measures were considered sufficient to provide 'more than minimal protection of confidential information' in the context of the use of such information by a large company with a significant turnover of employees. In addition, the trade secret holder

Copyright © Ana Rački Marinković

standard will necessarily change as technology evolves. This is a major concern when it comes to how firms manage cybersecurity threats: technical measures need to continually improve at speed, at least at the same pace as technologies used by criminals engaged in industrial espionage, hacking, and digital secret theft[42].

Protective measures in relation to employees are, as a rule, legal measures. Those employees who have to use trade secrets while performing their tasks must be legally obliged to keep them secret, and contractual responsibility in the case of infringement of the confidentiality obligation must be provided for. Employees also have to be trained in handling trade secrets; first of all, they must be made familiar with the foreseen measures of physical control and obliged to abide by them. A recent study confirms employee training as a protective measure which has been instituted in response to the Trade Secret Directive by some firms[43]. The identification of trade secrets in this context plays a significant role as an employee can undertake foreseen measures and keep information secret only if he is aware that this information is a trade-secret.

Measures of protection in respect of business partners are also legal, whether they appear as non-disclosure agreements or confidentiality clauses in other agreements. These measures also presuppose a clear designation of the information considered as a trade secret when disclosed to partners in business relationships. However, a Belgian lower court found that, even in the absence of an express contractual obligation, there was an implied duty of good faith in the contractual relationship between a company and an external consultant. Therefore, while contractual provisions are the most straightforward way to define protectable information, other context-specific commercial practices may satisfy the requirements for trade secret protection before the court[44]. Courts in the US were willing to imply a confidentiality obligation from the parties' relationship in several circumstances, such as, for example, joint ventures, business negotiations, license negotiations, vendor relationships, independent contractor relationships, and product sales[45].

4. COMPARING PROTECTIVE MEASURES IMPOSED BY THE GDPR AND THE TRADE SECRETS DIRECTIVE

There are obviously many differences as to the nature of the personal data and trade, some of which also impact the protective measures imposed by the GDPR and the Trade Secrets Directive. The laws that govern them comprise entirely different regimes, where the ratio of the protection of interest underlying them differs, as well as the consequences of not applying the appropriate protective measures.

While the GDPR and the Trade Secrets Directive originate from distinct legal philosophies, both frameworks are built upon the principle of neutrality, requiring organisations to adopt 'state-of-the-art' security measures that evolve alongside modern threats. Consequently, the technical and organisational steps taken to secure personal data often satisfy the 'reasonable steps' requirement for trade secret protection.

Table 1 summarizes these overlaps, demonstrating how a unified information governance strategy can efficiently address the mandates of both regimes.

Table 1

Identified overlapping of protective measures under GDPR[46] and Trade Secret Directive[47]
Organizational ● access policy ● decision on appointment of an authorized person/ data protection officer (GDPR) Physical: ● identity verification ● measures against unauthorized access, video-surveillance ● 'clean desk' policy, retention policies, and procedures

had also used an automatic backup procedure to avoid data loss, which was mentioned by the Court to show the company's diligence in its organisation of confidential information.

[42] *Ibid.* 66

[43] Aplin (n 1) 834

[44] European Union Intellectual Property Office (n 33) 68

[45] David W Quinto, Stuart H Singer, *Trade Secrets: Law and Practice* (2nd edn, Oxford University Press 2009) 14

[46] According to Sharma (n 15) 4, 10-11, 40

[47] According to De Vroey (n 14) 1-17

Copyright © Ana Rački Marinković

Legal:
- NDA

Security:
- firewalls, anti-virus software
- authentication tools
- password policy
- encryption

Trade secrets, like all other intellectual property, are private rights, so the promise of protection is given to foster innovation for the holder if he/she wants to make use of it. However valuable trade secrets may be, it is voluntary and up to the company to make use of the protection set up by the law, should they wish to. Companies may opt not to protect their trade secrets and may not impose any of the protective measures. As opposed to that, the protection of personal data derives from basic human rights to privacy, which are recognised and protected by law; therefore, it is mandatory for a company to introduce protective measures. When personal data forms part of trade secrets, those interests coincide.

However, should the company have an interest in protecting its trade secrets, the motive for establishing effective protective measures might be much higher than when protective measures are imposed under the GDPR to protect personal data. It is their advantage over the competitors that has commercial value that is protected, after all. Therefore, companies might not only introduce a 'minimum required' but also much more. Protective measures under the GDPR might be seen as a financial burden and a nuisance, with no imminent interest and a motive of the company to introduce them, apart from the fact that it is obliged to do so under the GDPR. The tendency to introduce the minimum required in order to meet the legal obligation is therefore expected. However, when personal data forms part of trade secrets, introducing higher levels of protective measures because of trade secrets protection will also benefit personal data.

The difference in consequence of not introducing adequate protective measures is also to be mentioned. If a company does not protect personal data and there is a data breach, the consequence for the company is that it will be fined, while the real loss in privacy will be suffered by the persons identified by these data. However, this does not destroy the privacy right as such; even if there is a breach in privacy and personal data is disclosed to others, the person remains in control of their personal data as such. It is often underlined as one of the disadvantages of trade secrets protection that, since it does not create an exclusive right, it will give its holder a factual monopoly as long as it remains secret. As opposed to infringements of intellectual property rights that do not affect the existence of a protected exclusive right, a trade secret, in being infringed, most often loses its factual monopoly and, with it, the possibility of further protection. In simple terms, once disclosed, the trade secret cannot become secret again. Thus, it loses the character of intellectual property, and, in relation to third parties, it becomes publicly available and can no longer provide any commercial advantage on the market to its holder. When personal data forms part of trade secrets, a breach in the protective measures that leads to personal data and trade secrets being disclosed to the public may destroy the secrecy and therefore the mere existence of such trade secrets in legal terms, while the data subject will still have the privacy right in respect of the personal data that was disclosed to others. Even more so, if protective measures are not judged as 'reasonable' in the circumstances of the case, since this is one element of the definition of trade secret, trade secrets will not be recognized as such. Not only the actual breach, but even the fact that measures might not be seen as reasonable, can therefore jeopardize legal protection of trade secrets. Providing an inadequate level of protective measures might therefore have greater repercussions in case of trade secrets.

Both in the case of trade secrets and in the case of personal data, the required level of protective measures depends on the circumstances of the case. While the evaluation in case of personal data will be performed by the administrative bodies in determining whether 'appropriate' measures were undertaken and impose fines if not, in case of trade secrets, the notion of 'reasonable' measures will be evaluated by the competent courts as one of the prerequisites for

Copyright © Ana Rački Marinković

granting trade secrets protection. However, both authorities may look into the decision of the other in evaluating the state of the art and the dynamics of the industry in determining what is reasonable or appropriate at a time, and their decisions of both may serve as guidance for the companies. Ideally, those standards would be uniform, since this would make it easier for companies to be able to introduce the same strategies in protecting both personal data and trade secrets. In practice, it is highly unlikely that a company would introduce, for example, a different level or system for encryption of data, whether it relates to personal data or to trade secrets, leading to a holistic information governance strategy that accounts for all types of information assets and their legal particularities[48]. This is even more so in cases when personal data forms part of trade secrets. Consequently, using the best practices to reduce the risk of exposure of or unauthorised access to both trade secrets and personal data will be required to comply with applicable legal requirements. But one also needs to be aware of the difference in threats that might influence the appropriate response of a company. Personal information is often targeted by criminal groups as part of ransomware attacks for monetary gain, whereas trade secrets are more often subject to cyber-misappropriation through advanced persistent threats, insider threats (e.g., employees), or through remote access tools[49].

Discussion of uniform protective measures for both personal data and trade secrets relates mainly to preventive security measures. In case of trade secrets, incident detection and the company's response do not, as in the case of private data breach, need to comply with the applicable legislation, as it is a private right. Remedies in case of unauthorised use of trade secrets under the Trade Secrets Directive are not aimed at preventing future breaches but compensating harm to the trade secret holder. However, the issue of a company's trade secret might arise when personal data breaches are investigated according to legal requirements. Forensic reports can contain, and if disclosed, have the potential to reveal information related to a company's trade secrets[50], particularly in cases where personal data forms part of trade secrets.

In addition to the similarity in types of protective measures to be included in protection programs encompassing technical, legal, and organisational measures (which include educating employees and developing an information-sensitive corporate culture), an important similarity is that protective measures in both cases need to be proactive. For trade secrets, it is of utmost importantance to first identify the trade secrets, while this, in legal terms, might not be as important for personal data. Personal data is legally defined, and this definition does not depend on the fact whether employees or third parties have been made aware of the fact that certain data amounts to personal data. Nevertheless, such 'data mapping' might also be needed in order to efficiently educate employees and should be a starting point for companies to develop their privacy policies[51], hence it is relevant for personal data as well. A thorough identification of trade secrets and personal data in a company might show that, because of their value, trade secrets may call for enhanced protective measures in comparison to personal data held by the company.

Finally, since studies show that mentioning the existence of trade secrets alone can attract cyber-attacks[52], trade secret protective measures are usually kept secret, like the secret information itself. Companies have few opportunities to learn about best practices in satisfying legal requirements on protecting trade secrets, except for available case law, which might be fragmented and inconsistent. There are, however, recognized certification opportunities and guidance from dedicated authorities and practice guides when it comes to personal data[53].

---

[48] Marek Nitoslawski, Eliane Ellbogen, 'From Personal Information to Trade Secrets Welcome to the Accelerated Digital Age!' <https://www.fasken.com/en/knowledge/2021/01/from-personal-information-to-trade-secrets-welcome-to-the-accelerated-digital-age> accessed 27 March 2026

[49] *Ibid.*<

[50] Tara Norgard, 'The Intersection of Trade Secrets and Data Privacy in the Digital Age' <https://www.bestlawyers.com/article/the-intersection-of-trade-secrets-and-data-pr/4891> accessed 27 March 2026

[51] Matthew Kohel, M., Austin Strine, 'Where Trade Secrets and Data Privacy Strategies Overlap' <https://ipwatchdog.com/2024/01/31/trade-secrets-data-privacy-strategies-overlap/> accessed 27 March 2026

[52] Michael Ettredge, Feng Guo, Yijun Li, 'Trade secrets and cyber security breaches' (2018) 37 (6) Journal of Accounting and Public Policy 585

[53] Nitoslawski (n 48)

Copyright © Ana Rački Marinković

This may be taken into account when setting strategies for protecting both personal data and trade secrets.

4.1. INTERRELATIONS BETWEEN PROVISIONS OF GDPR AND THE TRADE SECRET DIRECTIVE

Discussions about the prevalence of these rights are to be mentioned[54], mostly considering Article 15 (1) h of the GDPR, providing the right of access, which may be balanced with the rights and freedoms of others, including intellectual property and trade secrets. In its judgement in the case C-203/22[55] CJEU confirmed that such balancing must be carried out on a case-by-case basis (para. 75) so that the third-party personal data and controller's trade secrets "must be disclosed to the competent supervisory authority or court, which must balance the rights and interests at issue with a view to determining the extent of the data subject's right of access to personal data concerning him or her" (para. 74). Interrelationships between personal data and trade secrets is also found in recital 63 of the GDPR, referring that (the right of access "should not adversely affect the rights or freedoms of others, including trade secrets…") and in recital 34 and 35 of the Trade Secrets Directive, stating "this Directive respects the fundamental rights and observes the principles recognized in particular by the Charter, notably the right to respect for private and family life, the right to protection of personal data.."; "this Directive should not affect the rights and obligations laid down in [GDPR], in particular the rights of the data subject to access his or her personal data being processed and to obtain the rectification, erasure or blocking of the data where it is incomplete or inaccurate and, where appropriate, the obligation to process sensitive data in accordance with the [GDPR]". From the current state of law, and led by the logic of human rights, rights set forth under GDPR probably prevail against rights such as trade secrets. Therefore, the legitimate interest of the trade secret holder certainly has to be questioned in situations where data subjects are restricted in their rights.

5. CONCLUSION

Companies should reassess their data portfolio and, by objective criteria, classify personal data and other business data, including data with commercial value that can qualify as trade secrets. By identifying where personal identifiers and commercially sensitive secrets overlap, businesses can implement 'state-of-the-art' measures that satisfy both 'appropriateness' and 'reasonableness' standards simultaneously. This is because the GDPR and the Trade Secrets Directive, while emerging from distinct legal foundations, both request technical and organisational requirements for their implementation, which are essentially identical, as this study has demonstrated. This will allow organisations to adopt a holistic, uniform information governance model and avoid the traditional separation between personal data protection and trade secret preservation, which creates a significant regulatory disjunction and operational divergence within the modern corporate ecosystem. To map data within the system, business owners must become familiar with the regulatory framework, primarily the GDPR and Trade Secrets Directive (as well as the consequences of non-compliance with protective measures mandatory under the GDPR and required under the Trade Secrets Directive in order to claim legal protection). Trade secrets formed from the personal data must be protected and enclosed in accordance with both legislative frameworks. Besides non-compliance, the lack of awareness might be marked as a high risk. Therefore, a risk-based approach should be considered as a valuable tool to evaluate the appropriate level of organisational, technical, and security measures within the organisation and towards third parties, and the use of best practices for both personal data and trade secrets needs to be taken to reduce the risk. Establishing an integrated proactive security culture is not merely an operational efficiency but a legal necessity, and available case-law might serve as a guideline for choosing the appropriate level of protective measures depending on the circumstances of the case. Further studies may research the awareness of data holders of the obligation to conduct privacy risk assessments, as a first step in the implementation of the technical, organisational, and security measures. Also, it might be useful to research if trade secret holders are aware of the data protection rights, representing circumstances under which trade secrets may be disclosed.

REGULATIONS AND DOCUMENTS

1. European Union Intellectual Property Office: Trade secrets litigation trends in the EU, 2023. <https://www.euipo.europa.eu/en/publications/trade-secrets-litigation-trends-

[54] Custers (n 14) 1-17; Malgieri (n 14) 102–116

[55] Case C-203/22 *CK v Magistrat der Stadt Wien* [2025] ECR ECLI:EU:C:2025:117

Copyright © Ana Rački Marinković

in-the-eu>, last accessed on 02/06/2025.
2. Commission Staff Working Document: Impact assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, SWD [2013] 471, 113 <https:// eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013SC0471> accessed 27 March 2026
3. Directive (EU) 2016/943 of the European parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L 157/1
4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1
5. Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) [1994] Marrakesh Agreement Establishing the World Trade Organization, Annex 1C 1869 UNTS 299

JUDGMENTS AND OTHER DECISIONS

1. Case C-203/22 *CK v Magistrat der Stadt Wien* [2025] ECR ECLI:EU:C:2025:117
2. Case C-340/21 VB v Natsionalna agentsia za prihodite [2023] ECR ECLI:EU:C:2023:986
3. Case 2024-024797 *Autoriteit Persoonsgegevens v. HAN University of Applied Sciences* [2025] <https://autoriteitpersoonsgegevens.nl/system/files?file=2025-12/Boete%20HAN.pdf> accessed 27 March 2026
4. Case IMY-2025-7801 *The Swedish Authority for Privacy Protection (IMY) v. Sportadmin i Skandinavien AB* [2026] <https://www.imy.se/globalassets/dokument/tillsynsskrivelser/2026/beslut-efter-tillsyn-enligt-gdpr_sportadmin-i-skandinavien-ab.pdf> accessed 27 March 2026

INTERNET SOURCES

1. <https://www.edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en>, accessed 27 March 2026
2. <https://www.edpb.europa.eu/system/files/2025-03/edpb_summary_092022-012021_data_breach_en.pdf>, accessed 27 March 2026
3. Matthew Kohel, M., Austin Strine, 'Where Trade Secrets and Data Privacy Strategies Overlap' <https://ipwatchdog.com/2024/01/31/trade-secrets-data-privacy-strategies-overlap/> accessed 27 March 2026
4. Marek Nitoslawski, Eliane Ellbogen, 'From Personal Information to Trade Secrets Welcome to the Accelerated Digital Age!' <https://www.fasken.com/en/knowledge/2021/01/from-personal-information-to-trade-secrets-welcome-to-the-accelerated-digital-age> accessed 27 March 2026
5. Tara Norgard, 'The Intersection of Trade Secrets and Data Privacy in the Digital Age' <https://www.bestlawyers.com/article/the-intersection-of-trade-secrets-and-data-pr/4891> accessed 27 March 2026

BIBLIOGRAPHY

1. Tanya Aplin, Alfred Radauer, Martin A Bader, Nicola Searle, 'The Role of EU Trade Secrets Law in the Dana Economy: An Empirical Analysis' (2023) 54 (6) International Review of Intellectual Property and Competition Law 826-858.
2. Robert G Bone, 'Trade secrecy, innovation, and the requirement of

Copyright © Ana Rački Marinković

reasonable secrecy precautions' in Rochelle C Dreyfuss, Pauline Newman, Katherine J Strandburg (eds) *The law and theory of trade secrecy: a handbook of contemporary research* (Cheltenham 2012) 46-76

3. Mira Burri, Ingo Meitinger, 'The Protection of Undisclosed Information: Commentary of Article 39 TRIPS' in Thomas Cottier, Pierre Véron (eds) *Concise International and European IP Law: TRIPS, Paris Convention, European Enforcement and Transfer of Technology* (Kluwer Law International 2014) 1-6
4. Bart Custers, Anne-Sophie Heijne, 'The right of access in automated decision-making: The scope of Article 15(1)h GDPR in theory and practice' (2022) 46 Computer Law & Security Review 1-17
5. Michaël De Vroey, Margo Allaerts, 'Trade secrets protection: an interim update of Belgian and EU case law,' (2021) 16 (12) Journal of Intellectual Property Law & Practice 1391-1397
6. Michael Ettredge, Feng Guo, Yijun Li, 'Trade secrets and cyber security breaches' (2018) 37 (6) Journal of Accounting and Public Policy 564-585 https://doi.org/10.1016/j.jaccpubpol.2018.10.006
7. Lital Helman, 'Trade Secrets and Personal Secrets' University of Richmond Law Review (2021) 55 (2) 447-489
8. Gianclaudio Malgieri, 'Trade Secrets v Personal Data: A Possible Solution for Balancing Rights' (2016) 6 (2) International Data Privacy Law 102–116
9. Ulla-Maija Mylly, 'Trade Secrets and the Data Act' (2024) 55 (3) International Review of Intellectual Property and Competition Law 368-393
10. David Nguyen, Marta Paczos, 'Measuring the economic value of data and cross-border data flows: A business perspective' (2020) 297 OECD Digital Economy Papers <https://doi.org/10.1787/6345995e-en> accessed 27 March 2026
11. Pamela Samuelson, 'Privacy as Intellectual Property?' (2000) 52 (5) Stanford Law Review 1-42; Lital Helman, 'Trade Secrets and Personal Secrets' University of Richmond Law Review (2021) 55 (2) 447-489
12. Sharon K. Sandeen, 'Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law' (2006) 6 Michigan State Law Review 667-707
13. Sharon K Sandeen, 'The limits of trade secret law: Article 39 of the TRIPS Agreement and the Uniform Trade Secret Act on which it is based' in Rochelle C Dreyfuss, Pauline Newman, Katherine J Strandburg (eds) *The law and theory of trade secrecy: a handbook of contemporary research* (Cheltenham 2012) 537-567
14. Sanjay Sharma *Data Privacy and GDPR Handbook* (John Wiley & Sons 2020)
15. David W Quinto, Stuart H Singer, Trade Secrets: Law and Practice (2nd edn, Oxford University Press 2009).

Copyright © Ana Rački Marinković