Preliminary Communication
DOI: https://doi.org/10.22598/iele.2026.13.1.3

PURPOSE LIMITATION AND MACHINE LEARNING UNDER THE GDPR

Rastislav Funta [*]
Jörg Kohlenz [**]

ABSTRACT

When determining whether the use of machine learning is compliant with the GDPR, the trouble areas identified in standard big data studies are most affected. There are, however, unique characteristics that set machine learning apart from other large data analytics. The technological aspects of intelligent systems exacerbate the clash with the purpose restriction principle. This is related, on the one hand, to the fact that a machine learning model's processing processes are more sophisticated and hence more opaque than those of traditional algorithms, particularly in terms of transparency. On the other hand, it will be increasingly more unusual to presume that customer data was obtained specifically for the goal of training a machine learning model, necessitating a change of purpose even more frequently. This is especially true since it is already questionable whether the term "machine learning" can legitimately be used to define the goal of data processing. Based on this, the article investigates the research question of whether and to what extent machine learning may be applied in the sales industry while adhering to the GDPR's purpose limitation principle.

Key words: *GDPR, machine learning, personal data.*

1. INTRODUCTION

The principle of purpose limitation constitutes one of the structural cornerstones of the General Data Protection Regulation (GDPR). Pursuant to Article 5(1)(b) GDPR, personal data must be collected for specified, explicit, and legitimate purposes and must not be further processed in a manner incompatible

[*] Danubius University, Faculty of Law, Sládkovičovo, Slovakia, rastislav.funta@vsdanubius.sk

[**] Danubius University, Faculty of Public Policy and Public Administration, Sládkovičovo, Slovakia, kohlenz@kanzlei-kohlenz.de

with those purposes. At the same time, the GDPR does not impose an absolutely rigid prohibition on further processing, but rather establishes a framework in which purpose changes may be permitted under narrowly defined conditions, most notably through the compatibility test laid down in Article 6(4) GDPR. This regulatory architecture reflects an attempt to balance technological development and innovation with the protection of the fundamental rights to privacy and data protection guaranteed by Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union.[1]

The deployment of machine learning systems intensifies this balancing exercise. Unlike traditional data processing operations, machine learning relies on iterative, data-driven techniques that often generate new inferences from existing datasets and whose outcomes cannot be fully determined ex ante. This creates a structural tension with the GDPR's ex ante orientation towards clearly defined processing purposes. Legal scholarship has extensively analysed this tension in the broader context of big data analytics and artificial intelligence.[2] However, machine learning exhibits qualitative characteristics that exacerbate the conflict with purpose limitation beyond what is typically observed in classical statistical analysis. In particular, the opacity of model training processes, the reuse of datasets across different stages of the machine learning lifecycle, and the increasing practice of repurposing trained models for new commercial objectives raise specific challenges that existing doctrinal approaches do not sufficiently resolve.[3] This tension between advanced data analytics and purpose limitation has been identified in earlier scholarship on artificial intelligence and data protection, which already questioned whether traditional GDPR concepts can adequately constrain self-learning systems.

Early analyses emphasised that machine learning challenges the linear logic of data collection and use, particularly where algorithmic systems continuously recontextualise personal data beyond originally envisaged objectives. These concerns remain valid today and form an important backdrop for contemporary debates on AI governance under the GDPR. These challenges are particularly pronounced in the sales sector. Customer data used in sales environments—such as transaction histories, behavioural data, or loyalty programme

[1] Brkan, M.: The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. *German Law Journal*, 20(6) 2019, pp. 864-883.

[2] Kesa, A., Kerikmäe, T.: Artificial intelligence and the GDPR: Inevitable nemeses?. *TalTech Journal of European Studies*, 10(3) 2020, pp. 68-90.

[3] Mühlhoff, R., Ruschemeier, H.: Updating purpose limitation for AI: a normative approach from law and philosophy. *International Journal of Law and Information Technology,* 33 2025, pp. eaaf003.

information—are rarely collected with the explicit purpose of training machine learning models. Instead, controllers frequently seek to reuse already collected data for predictive analytics, personalised advertising, or customer profiling at a later stage. Empirical developments in digital commerce show that such secondary uses have become central to competitive strategy, while simultaneously increasing the risks of unlawful function creep.[4] This development is also reflected in empirical research on corporate data management practices. Studies of industrial and commercial enterprises demonstrate that personal and operational data are increasingly reused across organisational units and functional purposes, often without a clear ex ante limitation of secondary uses, thereby intensifying compliance challenges under the GDPR framework.[5] Recent case law of the Court of Justice of the European Union confirms that such secondary uses must be assessed in light of data subjects' reasonable expectations and the original context of data collection, even where advanced analytics are involved.[6] Moreover, the economic incentives driving the deployment of machine learning in sales must also be understood against the background of competition dynamics in digital markets. The concentration of data and the competitive advantages generated by predictive analytics reinforce pressures to reuse customer data beyond its initial purpose, intensifying the tension between data-driven innovation and legal constraints on purpose limitation.[7] Against this background, the legal uncertainty surrounding the qualification of "machine learning" itself as a sufficiently specific processing purpose becomes particularly salient. While technical literature often treats machine learning as a neutral methodology, GDPR compliance requires that purposes be formulated in a manner that allows data subjects to foresee the nature and extent of the processing.[8] It is therefore questionable whether references to model training or algorithmic optimisation can, in and of themselves, satisfy the requirements of Article 5(1)(b) GDPR. This question has gained renewed importance following the adoption of the EU Artificial Intelligence

[4] Mazurek, G.: Artificial Intelligence, Law, and Ethics. *Krytyka Prawa*, 15(1) 2023, pp. 11-14.

[5] Wallner, M., Peráček, T.: Data management in industrial companies: the case of Austria. *International Journal for Quality Research*, 17(3) 2023, pp. 847-866.

[6] Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 29 July 2019 – Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (Case C-40/17), 29.07.2019.

[7] Šmejkal, V.: Umělá inteligence jako kvalitativní výzva pro ochranu hospodářské soutěže. in: Mlsna, P. (ed.): *Hospodářská soutěž a veřejné zakázky. Synergie a průsečíky*, Plzeň: Aleš Čeněk, 2022, pp. 299-318.

[8] Becker, R., et al.: Purpose definition as a crucial step for determining the legal basis under the GDPR: implications for scientific research. *Journal of law and the biosciences*, 11(1) 2024, p. lsae001.

Act and the recent Opinion 28/2024 of the European Data Protection Board (EDPB), both of which emphasise the risks associated with secondary use of training data and AI models.[9]

The present article contributes to the existing literature by focusing specifically on the compatibility of machine learning applications in the sales sector with the purpose limitation principle under the GDPR. Unlike prior analyses that address artificial intelligence or machine learning in abstract or cross-sectoral terms, this article develops a doctrinal analysis centred on concrete sales-related use cases, such as customer profiling and targeted advertising. It also advances the discussion by conceptualising model training, validation, and application as legally distinct stages that may each trigger a change of purpose. In doing so, the article integrates recent CJEU jurisprudence, updated EDPB guidance, and the evolving EU digital regulatory framework in order to assess whether and under what conditions machine learning can be reconciled with the GDPR's purpose limitation principle in commercial practice.

2. AIM AND METHODOLOGY

The aim of this article is to examine whether, and under what conditions, machine learning can be lawfully applied in the sales sector in compliance with the GDPR's purpose limitation principle. The central research question is whether the further processing of personal data for machine learning purposes, particularly for model training, validation, and application in sales-related contexts, can be considered compatible with the purposes for which the data were originally collected within the meaning of Article 5(1)(b) GDPR. This analysis is conducted with particular emphasis on Article 6(4) GDPR, which constitutes the core legal mechanism for assessing the permissibility of changes in processing purposes.[10]

From a methodological perspective, the article adopts a doctrinal legal research approach. This approach is chosen deliberately, as the research question concerns the interpretation and systemic interaction of primary EU law (the Charter of Fundamental Rights of the European Union), secondary law (the GDPR and related digital legislation), and authoritative judicial and regulatory interpretations. Doctrinal analysis is particularly suitable where the

[9] European Data Protection Board: *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, Brussels: European Data Protection Board, 17.12.2024.

[10] Funta, R., Buttler, D.: The digital economy and legal challenges. *InterEULawEast*, 10(1) 2023, pp. 145-160.

objective is to clarify normative standards, resolve interpretative ambiguities, and assess internal consistency within a legal framework, rather than to empirically measure the effects of regulation. While empirical or interdisciplinary perspectives may complement doctrinal research, they are not indispensable for determining the legal limits of permissible data processing under Article 5 and Article 6 GDPR. The analysis focuses primarily on Articles 5(1)(b) and 6(4) GDPR, supplemented where necessary by Articles 6(1), 9, 14, 22, and 25 GDPR.

Particular attention is paid to the distinction between primary and secondary processing purposes and to the legal consequences of successive changes of purpose along the machine learning lifecycle. These provisions are interpreted in light of relevant recitals, notably Recitals 39 and 50 GDPR, which explicitly address foreseeability, reasonable expectations of data subjects, and further processing. In addition, the article systematically incorporates the jurisprudence of the Court of Justice of the European Union (CJEU) insofar as it clarifies core concepts such as personal data, controllership, legitimate expectations, and the limits of secondary use. Judgments including Nowak, Fashion ID, Jehovan Todistajat, and Meta Platforms Ireland are used not as isolated authorities but as part of a coherent interpretative framework that informs the application of purpose limitation and compatibility in technologically complex settings.[11] These cases are particularly relevant because they demonstrate the Court's functional and context-oriented approach to data protection concepts, which is essential when assessing machine learning in sales environments. Furthermore, the article relies on guidance issued by the European Data Protection Board (EDPB) and its predecessor, the Article 29 Working Party. While such guidance is not legally binding, it plays a central role in shaping supervisory practice and provides an authoritative interpretation of GDPR provisions relevant to profiling, further processing, and automated decision-making. In particular, EDPB Guidelines on consent, targeting, data protection by design, and the recent Opinion 28/2024 on AI models are taken into account.[12] These doc-

[11] Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 20 December 2017 – Peter Nowak v Data Protection Commissioner (Case C-434/16), 20.12.2017; Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 10 July 2018 – Tietosuojavaltuutettu v Jehovan todistajat – uskonnollinen yhdyskunta (Case C-25/17), 10.07.2018; Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 29 July 2019 – Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (Case C-40/17), 29.07.2019; Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 4 July 2023 – Meta Platforms Inc. and Others v Bundeskartellamt (Case C-252/21), 04.07.2023.

[12] European Data Protection Board: *Guidelines 8/2020 on the targeting of social media users*, Brussels: European Data Protection Board, 13.4.2021; European Data Protection Board:

uments are selected because they directly address the risks of function creep, secondary use of data, and the reuse of trained models - issues that are pivotal for machine learning applications in sales. Methodologically, the article combines this doctrinal analysis with a structured conceptual examination of the machine learning lifecycle. Instead of treating "machine learning" as a monolithic processing operation, the analysis differentiates between preprocessing, model training, validation, testing, and model application. This differentiation is not technical for its own sake but serves to identify where legally relevant changes of purpose may occur. From a technical perspective, such multi-stage models of data analysis are well documented in applied research on user data processing and web-based projects, which emphasise iterative reuse of datasets across different functional objectives and operational contexts.[13]

The interaction between technical process stages and legal purpose definitions constitutes a central analytical lens of the article. While the article does not include empirical case studies or quantitative analysis, it uses illustrative sales-related examples, such as customer profiling and targeted advertising, to concretise abstract legal standards. The resulting analysis aims to contribute to both academic discourse and legal practice by clarifying how the compatibility test under Article 6(4) GDPR can be operationalised in the sales sector without undermining the fundamental role of the purpose limitation principle. The doctrinal methodology adopted in this article also reflects a broader debate in data protection scholarship concerning the normative strength of purpose limitation as a fundamental rights safeguard. Some authors warn against reducing purpose limitation to a purely formal compliance requirement, arguing instead that it constitutes a structural guarantee against the erosion of individual autonomy in data-driven societies. Others emphasise the need for interpretative flexibility to ensure effective governance of emerging technologies. This tension is addressed in the present analysis by interpreting Article 6(4) GDPR as a constrained flexibility mechanism rather than a deregulatory gateway.[14]

Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1, Brussels: European Data Protection Board, 4.5.2020.

[13] Fedushko, S., et al.: Model of user data analysis complex for the management of diverse web projects during crises. *Applied Sciences*, 10(24) 2020, pp. 1-12.

[14] van der Sloot, B.: Legal fundamentalism: is data protection really a fundamental right?. in: Leenes, R., et al. (eds.): *Data protection and privacy: (in)visibilities and infrastructures*, Heidelberg: Springer, 2017, pp. 3-30.

3. THE MANNER OF PROCESSING

The concept of the "manner" of processing, as referred to in Article 5(1)(b) GDPR, must not be misconstrued as introducing an additional or autonomous processing requirement beyond the determination of processing purposes. Regarding the purpose limitation principle, the decisive criterion remains whether personal data are further processed for a purpose that differs from the purpose for which they were originally collected and, if so, whether this further purpose is compatible with the original one. The wording of Article 5(1)(b) GDPR should therefore not be interpreted as prohibiting further processing for the same purpose solely because technical or organisational circumstances of the processing have changed. At the same time, the GDPR systematically links the "manner" of processing to the overall processing operation in a broad and functional sense. Article 5(1)(a) GDPR requires that personal data be processed "lawfully", while Article 5(1)(f) GDPR refers to processing "in a manner that ensures appropriate security". Even more explicitly, Article 4(2) GDPR defines processing as "any operation or set of operations" performed on personal data, covering both manual and automated means. This understanding is confirmed by provisions such as Article 4(12) GDPR, which defines a personal data breach by reference to the way in which data are processed, and Article 17(1)(a) GDPR, which links erasure to the necessity of data "in relation to the purposes for which they were collected or otherwise processed".[15] From this systemic perspective, the "manner" of processing does not introduce a separate normative category, but rather describes the technical and organisational realisation of a given processing purpose.

The relevance of technical processing characteristics must also be assessed in light of the concept of identifiability. The Court of Justice has clarified that the qualification of information as personal data does not depend solely on whether identification is immediate, but on whether identification is reasonably likely in light of available means. This interpretation is particularly relevant for machine learning systems, where model outputs or derived datasets may allow indirect re-identification of data subjects.[16] Supervisory authorities have similarly emphasised that technological context and realistic re-identification risks must be taken into account when assessing compliance with the GDPR's

[15] Custers, B., Malgieri, G.: Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data. *Computer Law & Security Review*, 45(July) 2022, pp. 1-13.

[16] Tzanou, M.: Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection. *Croatian Yearbook of European Law & Policy*, 6(1) 2010, pp. 53-74.

core principles.[17] Consequently, Article 5(1)(b) GDPR is best understood as establishing a two-step assessment: first, the controller must determine whether the contemplated processing operation pursues a purpose that is different from the purpose of collection; second, if this is the case, the controller must assess whether the manner in which the data are processed for this new purpose remains compatible with the original purpose. This interpretation is consistent with Recital 39 GDPR, which emphasises that personal data should be processed in a way that is foreseeable for data subjects and limited to what is necessary in relation to the purposes pursued.[18]

In the context of machine learning, this distinction acquires particular significance. Machine learning does not merely involve a change in technical tools but often entails a qualitative transformation of the processing operation itself. The reuse of customer data for model training, pattern recognition, or predictive analytics typically pursues a different objective than the original collection purpose, such as contract execution or service provision. In sales environments, for example, customer address data collected for product delivery may later be reused to train recommender systems or customer profiling models. Even if the underlying data fields remain unchanged, the processing purpose is no longer identical, triggering the applicability of the purpose limitation principle. Recent CJEU case law supports a functional, context-sensitive approach to determining when such qualitative changes amount to a new processing purpose. In Nowak, the Court emphasised that the scope of data protection depended on the use and potential impact of data processing, not merely on formal classifications of processing operations.[5] Similarly, in Fashion ID, the Court made clear that the definition of processing purposes must take account of how data are actually used within a broader processing architecture, particularly where multiple actors or processing stages are involved.[19] These insights are directly applicable to machine learning pipelines in sales, where preprocessing, model training, and model application may involve distinct legal evaluations. EDPB guidance reinforces this approach by highlighting the risk of "function creep" where data collected for one purpose are gradually repurposed for additional objectives without adequate legal justification. The EDPB has repeatedly stressed that changes in processing operations characterised by

[17] Siwicki, M.: Big Data Profiling and Predictive Analytics from the Perspective of GDPR. *Studia Iuridica Lublinensia*, 32(2) 2023, pp. 249-266.

[18] Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 20 December 2017 – Peter Nowak v Data Protection Commissioner (Case C-434/16), 20.12.2017.

[19] Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 29 July 2019 – Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (Case C-40/17), 29.07.2019.

advanced analytics or profiling cannot be justified merely by their technical sophistication, but must always be assessed against the originally specified purpose.[20] This is particularly relevant in sales contexts, where machine learning systems are increasingly deployed to infer customer preferences, predict purchasing behaviour, or personalise advertising, thereby deepening the impact on data subjects' rights and expectations. Accordingly, a processing purpose is "different" within the meaning of Article 5(1)(b) GDPR whenever it is not fully identical to the purpose for which the data were originally collected, regardless of whether the same technical data are reused. The decisive element is not the continuity of the dataset, but the shift in the objective pursued by the controller. This interpretation ensures internal consistency within the GDPR's normative framework and prevents controllers from circumventing the purpose limitation principle by framing extensive machine learning operations as mere technical variations of existing processing activities.

4. REFERENCE POINT FOR COMPATIBILITY OF PURPOSES

The assessment of whether a further processing purpose is compatible with the purpose for which personal data were originally collected requires, as a preliminary step, a clear determination of the relevant reference point. Article 5(1)(b) GDPR prohibits further processing that is incompatible with the purposes of collection, while Article 6(4) GDPR specifies criteria for determining compatibility. Both provisions presuppose a comparison between at least two purposes. The decisive question is therefore which purposes are to be compared when assessing compatibility, particularly in complex processing chains such as the characteristics of the machine learning lifecycle. The answer is straightforward in scenarios involving a single change of purpose. Where personal data collected for one purpose, such as fulfilling a sales contract, are later reused for another purpose, such as training a customer profiling model - the original purpose of collection and the newly introduced processing purpose constitute the relevant comparison pair. In sales environments, this constellation is typical: customer data initially collected for order processing or customer service are subsequently repurposed for predictive analytics, personalised marketing, or demand forecasting. In such cases, the compatibility assessment under Article 6(4) GDPR must clearly relate the secondary purpose to the original purpose of collection. Greater conceptual difficulty arises where

[20] European Data Protection Board: *Guidelines 8/2020 on the targeting of social media users*, Brussels: European Data Protection Board, 13.4.2021; European Data Protection Board: *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, Brussels: European Data Protection Board, 17.12.2024.

multiple successive changes of purpose occur. Machine learning applications routinely involve several stages, such as model training, validation, testing, and application, and data may be reused across these stages or even across different models. It is therefore conceivable that personal data are first repurposed from their original collection purpose to train a machine learning model and subsequently reused to train another model or to support a different commercial objective. This raises the question of whether, in the case of such tertiary processing purposes, compatibility should be assessed against the immediately preceding secondary purpose or against the original purpose of collection. A systematic interpretation of Article 5(1)(b) and Article 6(4) GDPR indicates that the only legally relevant reference point remains the original purpose of data collection. Both provisions consistently refer to compatibility with "the purposes for which the personal data were collected", not to purposes defined at later stages of processing. The same applies to Recital 39 GDPR, which emphasises foreseeability and transparency "at the time of collection", as well as to Recital 50 GDPR, which frames further processing in relation to the original purpose. This linguistic consistency across the GDPR versions supports the conclusion that even tertiary purposes must ultimately be measured against the initial collection purpose. This interpretation is further reinforced by the broader normative context of the GDPR.

Purpose specification at the time of data collection is intended to delineate a legally permissible processing framework within which the controller may operate. If compatibility were assessed only in relation to the immediately preceding purpose, controllers could continuously redefine the benchmark for further processing through successive purpose changes, thereby undermining the protective function of the purpose limitation principle. Such an approach would expose data subjects to an open-ended chain of foreseeable processing operations, rendering meaningful consent and predictability illusory.[21] These considerations are reinforced by broader analyses of digital communication environments, which emphasise that users' expectations regarding data use are shaped by the communicative context and perceived function of online services. Where data are collected in environments primarily understood as transactional or communicative, extensive analytical reuse may exceed what data subjects reasonably anticipate.[22] CJEU jurisprudence supports this under-

[21] Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 19 October 2016 – Patrick Breyer v Bundesrepublik Deutschland (Case C-582/14), Judgment of 19.10.2016; Fedushko, S., et al.: Model of user data analysis complex for the management of diverse web projects during crises. *Applied Sciences*, 10(24) 2020, pp. 1-12.

[22] Šramel, B., Horváth, P.: Internet as the communication medium of the 21st century: do we need a special legal regulation of freedom of expression on the internet. *The Lawyer Quarterly*, 11(1) 2021, pp. 141-157.

standing by consistently emphasising the centrality of the original collection context and the reasonable expectations of data subjects. In Jehovan Todistajat, the Court linked the scope of permissible processing to the circumstances under which the data were initially obtained.[23] Similarly, in Fashion ID, the Court highlighted that controllership and purpose determination must be assessed in light of the role played at the point where data processing is initiated, rather than retrospectively redefined by downstream processing activities.[24]

More recently, the Court in Meta Platforms Ireland reaffirmed that secondary uses of personal data - particularly in advertising and profiling contexts - must remain within the limits established by the original collection purpose and the expectations derived therefrom.[25] EDPB guidance aligns with this approach. The EDPB has repeatedly stressed that compatibility assessments must not be used to legitimise uncontrolled "function creep", especially in contexts involving profiling, behavioural prediction, or AI-driven decision-making. The Opinion 28/2024 on AI models explicitly warns against the reuse of training data or trained models for new purposes without reassessing their compatibility with the original collection purposes. This guidance is particularly relevant for machine learning in sales, where economic incentives may favour extensive reuse of datasets and models across different commercial functions. From a functional perspective, anchoring the compatibility assessment to the original purpose of collection also ensures verifiability and enforceability of GDPR compliance. Only at the moment of data collection can the data subject meaningfully influence whether and under what conditions their data are processed. The purpose specified at that stage provides the reference framework for assessing later processing operations, determining storage limitation under Article 5(1)(e) GDPR, and triggering erasure obligations under Article 17 GDPR. Allowing this reference framework to shift dynamically through purpose redefinitions would be incompatible with the GDPR's rights-based architecture. Accordingly, even in complex machine learning lifecycles involving multiple processing stages, all secondary and tertiary processing purposes must ultimately be assessed for compatibility with the original purpose of data collection. This conclusion does not preclude further processing in principle, but it sets a stable and foreseeable benchmark against which such processing

[23] Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 10 July 2018 – Tietosuojavaltuutettu v Jehovan todistajat – uskonnollinen yhdyskunta (Case C-25/17), 10.07.2018.

[24] Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 29 July 2019 – Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (Case C-40/17), 29.07.2019.

[25] Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 4 July 2023 – Meta Platforms Inc. and Others v Bundeskartellamt (Case C-252/21), 04.07.2023.

must be evaluated. It thereby preserves the integrity of the purpose limitation principle while allowing for controlled flexibility under Article 6(4) GDPR.

5. PRIVILEGING OF PROCESSING OPERATIONS PURSUANT TO ARTICLE 89 GDPR

Article 5(1)(b), second sentence, GDPR, introduces an exception to the purpose limitation principle by providing that further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered incompatible with the initial purposes, provided that appropriate safeguards are applied in accordance with Article 89(1) GDPR. This provision establishes a form of normative privileging, whereby certain secondary processing operations are deemed compatible by legal fiction and therefore do not require a compatibility assessment under Article 6(4) GDPR. The legislative history of the GDPR demonstrates that this privileging is not intended merely as a rebuttable presumption of compatibility, but rather as a binding legal classification. If the drafters had intended the compatibility of these purposes to be assessed on a case-by-case basis, the relevant rule could have been confined to the recitals. Instead, it was incorporated into the normative text of the Regulation, thereby granting scientific research and statistical processing a structurally privileged status within the GDPR framework. The consequence is that controllers engaging in such processing are exempted from the compatibility test, although they remain bound by the general principles of data protection, including data minimisation, security, and transparency. Despite this apparent clarity, the scope and rationale of the privilege remain contested. A prevailing view explains the privilege by reference to the fact that, in genuine research and statistical contexts, personal data are not processed with the aim of affecting or evaluating individual data subjects, but are instead used as an abstract informational basis to generate generalisable knowledge. Other approaches conceptualise Article 5(1)(b), second sentence, GDPR as a narrow exception to be interpreted restrictively in light of the fundamental importance of purpose limitation. These doctrinal uncertainties become particularly salient when controllers seek to rely on Article 89 GDPR to justify machine learning applications outside traditional research environments.

In the context of machine learning, the potential relevance of Article 89 GDPR must therefore be assessed with caution. While machine learning is often associated with knowledge generation and pattern discovery, this does not automatically qualify such processing as "scientific research" within the meaning of the GDPR. Recital 159 GDPR requires that scientific research be interpreted

broadly, including technological development, but this cannot be understood as encompassing all forms of data-driven innovation. Otherwise, large parts of commercial analytics and intelligent systems deployment would be effectively exempted from the purpose limitation principle, contrary to its central position in the GDPR's normative architecture. This concern is particularly acute in the sales sector. Machine learning applications in sales, such as recommendation engines, pricing optimisation, or targeted advertising, are typically designed to influence individual consumer behaviour and to improve commercial performance. The processing purpose therefore relates directly to identifiable data subjects and their economic decisions, rather than to the production of generalisable knowledge for societal benefit. Even where insights are derived at an aggregate level, the ultimate objective remains the optimisation of individual-level interactions with customers.[26] As a result, reliance on Article 89 GDPR in such contexts would stretch the provision beyond its intended scope. EDPB guidance supports a restrictive interpretation of the research privilege in this regard. The EDPB has emphasised that the classification of processing as "scientific research" requires an assessment of the processing purpose, governance framework, and safeguards, and cannot be based solely on the use of advanced analytical techniques. The Opinion 28/2024 on AI models further reinforces this position by warning against the assumption that training or deploying AI models automatically falls outside the scope of purpose limitation due to alleged anonymisation or research characteristics. Instead, controllers must carefully assess whether personal data processing remains linked to identifiable individuals and whether outputs are reused for new, non-research purposes.[27] The same reasoning applies to the privileging of statistical purposes. While certain machine learning operations may produce statistical outputs, this does not suffice to trigger the privilege where such outputs are subsequently used for decision-making or profiling at the individual level. Article 89 GDPR presupposes that appropriate safeguards, such as pseudonymisation and purpose separation, are implemented precisely to prevent the reidentification or individualised use of data. In sales-related machine learning applications, however, the value of the system often lies precisely in its capacity to act upon individual customer profiles, thereby precluding reliance on the statistical privilege.[28] Accordingly, actors operating within the machine learning lifecy-

[26] Siwicki, M.: Big Data Profiling and Predictive Analytics from the Perspective of GDPR. *Studia Iuridica Lublinensia*, 32(2) 2023, pp. 249-266.

[27] European Data Protection Board: *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, Brussels: European Data Protection Board, 17.12.2024.

[28] Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 4 July 2023 – Meta Platforms Inc. and Others v Bundeskartellamt (Case C-252/21), 04.07.2023.

cle in the sales sector cannot reliably invoke Article 89 GDPR to bypass the compatibility requirements of Article 5(1)(b) and Article 6(4) GDPR. While specific machine learning projects conducted strictly for scientific research purposes, such as consumer behaviour studies carried out under robust governance frameworks and without commercial exploitation, may fall within the scope of the privilege, such scenarios constitute exceptions rather than the rule. For most sales-related applications, the permissibility of further processing must therefore be assessed through the compatibility test set out in Article 6(4) GDPR, rather than through recourse to the research and statistics privilege.

6. CLARIFICATION OF LEGAL CHANGES TO THE PROCESSING PURPOSES THROUGH ARTICLE 6 PARA. 4 GDPR

Where machine learning is employed in the sales sector, the permissibility of changing processing purposes cannot generally be derived from the privileging mechanisms of Article 5(1)(b), second sentence, GDPR, nor from Union or Member State law within the meaning of Article 23 GDPR. As demonstrated above, consent likewise fails to provide a stable basis for most machine-learning-related purpose changes due to its strict requirements of specificity and foreseeability. Consequently, Article 6(4) GDPR emerges as the central legal mechanism for assessing whether the further processing of personal data for machine learning purposes may take place in compliance with the purpose limitation principle. Article 6(4) GDPR fulfils a specific and circumscribed function within the normative framework of the GDPR. It does not relax the requirement of lawfulness under Article 5(1)(a) GDPR, nor does it create an autonomous legal basis for further processing. Rather, it concretises the abstract prohibition of incompatible further processing under Article 5(1)(b) GDPR by specifying the conditions under which a modified processing purpose may still be regarded as compatible with the purpose of collection. This distinction between the acceptability of a change of purpose and the lawfulness of the processing operation is fundamental, particularly in data-intensive environments characterised by iterative reuse of personal data, such as machine learning in sales contexts.

6.1. THE COMPATIBILITY TEST AS A STRUCTURED BALANCING EXERCISE

The compatibility test laid down in Article 6(4) GDPR requires an evaluative assessment of several mandatory criteria: the link between the original and new purposes, the context in which the data were collected, the nature of the

personal data concerned, the possible consequences for data subjects, and the safeguards implemented by the controller. These criteria must be assessed cumulatively and in light of the reasonable expectations of data subjects, as emphasised in Recital 50 GDPR.[29] The test thus embodies a structured balancing of interests that seeks to protect data subjects from unforeseeable expansions of data use while allowing limited flexibility for legitimate secondary processing. In this respect, the compatibility test resembles but must be clearly distinguished from the balancing exercise under Article 6(1)(f) GDPR. While both mechanisms involve competing interests, Article 6(4) GDPR operates exclusively at the level of purpose limitation. It presupposes that both the original and the intended further processing are, in principle, capable of being lawful. The test does not determine whether the processing may take place at all, but whether the controller may depart from the originally specified purpose without violating the GDPR's ex ante protective logic.

The assessment of safeguards under Article 6(4)(e) GDPR must also be understood in a broader governance and security context. Recent scholarship emphasises that, in AI-driven environments, purpose limitation cannot be effectively safeguarded without integrated cybersecurity and data protection measures that address risks arising from data aggregation, model inference, and system interoperability. A holistic approach to data governance, combining technical, organisational, and legal safeguards, therefore plays a crucial role in mitigating the risks associated with secondary data use in machine learning systems.[30] CJEU jurisprudence confirms the autonomy of the purpose limitation principle in this regard. In Meta Platforms Ireland, the Court made clear that secondary uses of personal data for personalised advertising and profiling must remain closely connected to the original context of data collection and the legitimate expectations of data subjects. Similarly, earlier cases, such as Jehovan Todistajat, demonstrate that compatibility assessments must be anchored in the initial circumstances under which the data were obtained, rather than being redefined dynamically by subsequent processing stages. These findings are directly relevant for machine learning applications in sales, where data collected for transaction execution or customer accounts are later reused for predictive analytics.

[29] European Data Protection Board: *Guidelines 8/2020 on the targeting of social media users*, Brussels: European Data Protection Board, 13.4.2021.

[30] Karpiuk, M., Melchior, C., Kaczmarek, K.: A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data. *Prawo i Więź*, 50(3) 2024, pp. 104-121.

6.2. LIMITED ROLE OF LEGISLATION AND CONSENT

Article 6(4) GDPR allows further processing for incompatible purposes only where it is based on Union or Member State law pursuant to Article 23 GDPR or on the consent of the data subject. In the sales sector, neither pathway offers a viable general solution. Commercial objectives such as marketing optimisation or customer segmentation cannot plausibly be characterised as pursuing important objectives of general public interest within the meaning of Article 23 GDPR, without fundamentally diluting the restrictive nature of that provision.[31] Consent, while theoretically available, is structurally ill-suited to the machine learning lifecycle. Valid consent requires that data subjects are informed of specific processing purposes and can reasonably foresee the consequences of data use. Where machine learning systems are deployed to explore correlations, generate predictions, or continuously refine models, such foreseeability is often absent. As a result, consent is prone to either excessive abstraction or subsequent invalidity. Both the EDPB and recent academic analyses have stressed that consent must not be instrumentalised as a corrective mechanism for insufficient purpose specification or accountability.[32] This conclusion is further supported by analyses of the evolving regulatory obligations imposed on EU Member States in the field of artificial intelligence. Recent findings highlight that, notwithstanding the increasing density of AI-specific regulation, Member States remain bound to ensure the effective application of existing data protection principles, including purpose limitation, within their domestic legal orders. The emergence of new AI governance frameworks therefore does not displace Article 6(4) GDPR, but rather increases the need for coherent interpretation and enforcement across regulatory layers.

6.3. NECESSITY OF AN INDEPENDENT LEGAL BASIS FOR FURTHER PROCESSING

A central doctrinal controversy concerns whether a successful compatibility assessment under Article 6(4) GDPR obviates the need for a separate legal basis under Article 6(1) GDPR. This chapter endorses the position consistently taken by supervisory authorities and supported by systematic interpretation: Article 6(4) GDPR does not itself constitute a legal basis for further processing. Compatibility of purpose and lawfulness of processing are cumulative

[31] Napieralski, A.: Between the Data Act and the GDPR: Attributing Responsibility for Data Sharing. *Yearbook of Antitrust and Regulatory Studies*, 17(29) 2024, pp. 127-145.

[32] European Data Protection Board: *Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1*, Brussels: European Data Protection Board, 4.5.2020.

requirements. This conclusion follows directly from the structure of the GDPR and from Article 8(2) of the Charter of Fundamental Rights of the European Union, which requires that personal data be processed for specified purposes and on a legitimate legal basis. The use of the conjunction "and" indicates that these safeguards operate independently. Article 6(4) GDPR governs only the former by delimiting the permissible scope of purpose changes; it does not legitimise the corresponding interference with fundamental rights. Allowing compatibility to substitute for a legal basis would undermine the principle of legality in Article 5(1)(a) GDPR and run counter to the requirement of clarity and predictability of legal bases emphasised in Recital 41 GDPR.

6.4. APPLICATION TO MACHINE LEARNING IN THE SALES SECTOR

When applied to machine learning in sales environments, this cumulative structure means that controllers must satisfy two distinct conditions when reusing customer data for model training or application: the new processing purpose must be compatible with the purpose of collection, and the processing must be supported by a valid legal basis under Article 6(1) GDPR. For example, reusing transaction data collected for order fulfilment to train a recommendation system aimed at targeted advertising constitutes a change of purpose that must be carefully assessed under Article 6(4) GDPR. The more such systems are designed to influence individual behaviour or generate individual-level predictions, the stricter the compatibility assessment must be. This interpretation preserves the preventive and rights-protective function of the purpose limitation principle without rendering machine learning impermissible per se. Article 6(4) GDPR does not prohibit innovation, but it requires that innovation take place within a bounded and foreseeable purpose framework. In this sense, the compatibility test acts as a normative bridge between classical data protection concepts and emerging forms of algorithmic processing. Recent research on AI governance confirms that maintaining such boundaries is essential to prevent the erosion of individual autonomy and informational self-determination in commercial data ecosystems.[33] In this context, it should be noted that conformity assessment mechanisms under the AI Act are designed to ensure technical and organisational compliance of high-risk systems, but they do not address the lawfulness of personal data reuse under the GDPR. As recent commentary highlights, AI Act conformity assessments and GDPR purpose limitation operate on different normative levels and must be fulfilled

[33] Vardanyan, L., Stehlík, V., Kocharyan, H.: Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity. *TalTech Journal of European Studies*, 12(1) 2022, pp. 159-185.

cumulatively rather than alternatively.[34] These considerations are particularly relevant where machine learning systems are deployed within complex digital ecosystems involving multiple actors, such as online platforms or integrated sales infrastructures. In such environments, determining responsibility for purpose definition and further processing becomes a distributed exercise. The Court of Justice has repeatedly underlined that the allocation of responsibility under the GDPR must reflect actual influence over purposes and means of processing, even where technical control is shared.[35] Moreover, fundamental-rights limitations remain applicable irrespective of economic or structural constraints arising from platform-based business models.[36] From a regulatory perspective, these findings reinforce the importance of embedding purpose limitation and compatibility considerations into system design, as required by the principle of data protection by design and by default.[37]

7. CONCLUSION

This article has demonstrated that the application of machine learning in the sales sector is not per se incompatible with the GDPR's purpose limitation principle. Nevertheless, the use of such technologies significantly narrows the margin of legally permissible data processing and requires a carefully structured assessment of purpose specification and purpose change. While preprocessing operations and the use of model outputs that directly correspond to the original collection purpose generally do not raise insurmountable concerns under Article 5(1)(b) GDPR, the decisive legal challenges arise at later stages of the machine learning lifecycle, particularly during model training, validation, and testing. A central finding of this analysis is that machine learning cannot, in itself, be regarded as a sufficiently specific processing purpose within the meaning of the GDPR. The indeterminacy of model outcomes and the exploratory nature of many machine learning techniques prevent controllers from defining, at the time of collection, the scope and consequences of future processing with the precision required by Article 5(1)(b) GDPR. This applies

[34] Szuchy, R.: Conformity assessments under the EU AI Act: Ensuring compliance, safety and trust in artificial intelligence. *Legal Business*, 2024, pp. 56-57.

[35] Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 5 June 2018 – Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (Case C-210/16), 05.06.2018.

[36] Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 16 July 2020 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Case C-311/18), 16.07.2020.

[37] European Data Protection Board: *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, Brussels: European Data Protection Board, 20.10.2020.

with particular force in sales-related contexts, where machine learning is used for predictive profiling, personalised advertising, or behavioural targeting. As a result, the deployment of such systems typically entails one or more changes of purpose that trigger the application of Article 6(4) GDPR.

The article further confirms that Article 6(4) GDPR constitutes the central legal mechanism through which purpose changes in the machine learning lifecycle must be assessed. The compatibility test prescribed therein functions as a structured balancing exercise that preserves the ex ante protective logic of the purpose limitation principle while providing limited flexibility for technological innovation. Importantly, however, a successful compatibility assessment does not itself render further processing lawful. Controllers must additionally rely on an independent legal basis under Article 6(1) GDPR. This cumulative requirement follows from the GDPR's internal structure and from Article 8(2) of the Charter of Fundamental Rights of the European Union, and has been consistently affirmed by supervisory authorities and recent findings.[38] The article has also shown that commonly invoked alternative pathways, such as reliance on consent or on the research and statistics privilege under Article 89 GDPR, are of limited relevance in the sales sector. Due to the specificity and foreseeability requirements associated with valid consent, and the individually targeted nature of sales-oriented machine learning, these mechanisms cannot ordinarily compensate for deficiencies in purpose specification. Recent EDPB guidance on AI models confirms that neither anonymisation claims nor references to innovation or technical development can justify unrestrained secondary use of personal data or trained models. From a practical perspective, the findings imply that controllers seeking to deploy machine learning systems in sales environments must integrate purpose limitation assessments into the design and governance of the machine learning lifecycle.[39] This includes identifying potential purpose changes at an early stage, minimising the scope of training data, implementing technical and organisational safeguards, and documenting compatibility assessments in a manner that is verifiable by supervisory authorities. Approaches such as incremental model development, data quality optimisation, and strict separation of training and application purposes may mitigate conflicts with Article 5(1)(b) GDPR without precluding the use of intelligent systems altogether.

The analysis is subject to certain limitations. It adopts a doctrinal legal methodology and does not empirically assess how controllers operationalise purpose limitation in practice, nor does it offer a comparative analysis with non-EU data

[38] Becker, R., Chokoshvili, D., Dove, E. S.: Purpose limitation and secondary use of personal data in AI-driven research after GDPR: unresolved tensions. *International Data Privacy Law*, 14(3) 2024, pp. 1-18.

[39] Napieralski, A.: Between the Data Act and the GDPR: Attributing Responsibility for Data Sharing. *Yearbook of Antitrust and Regulatory Studies*, 17(29) 2024, pp. 127-145.

protection regimes. Moreover, regulatory developments such as the AI Act and the Data Act, while already influential, have not yet been fully tested through enforcement practice or judicial interpretation. Future research could therefore benefit from empirical case studies, interdisciplinary perspectives, and a closer examination of how emerging digital regulations interact with the GDPR's purpose limitation principle in concrete commercial settings. In conclusion, machine learning can be reconciled with the GDPR's purpose limitation principle in the sales sector only if controllers accept that technological capability does not equate to legal permissibility. Article 6(4) GDPR provides a narrowly circumscribed space within which purpose changes may occur, but it does not dilute the fundamental requirement that data subjects remain protected against unforeseeable and uncontrolled secondary uses of their personal data. The continued relevance of purpose limitation in the age of machine learning thus lies not in resisting technological change, but in ensuring that such change unfolds within a legally bounded and rights-respecting framework.

LITERATURE

1. Becker, R., Chokoshvili, D., Dove, E. S.: Purpose limitation and secondary use of personal data in AI-driven research after GDPR: unresolved tensions. *International Data Privacy Law*, 14(3) 2024, pp. 1-18.
   - DOI: https://doi.org/10.1093/idpl/ipae014
2. Becker, R., Chokoshvili, D., Thorogood, A., Dove, E. S., Molnar-Gabor, F., Ziaka, A., Tzortzatou, O., Comandè, G.: Purpose definition as a crucial step for determining the legal basis under the GDPR: implications for scientific research. *Journal of law and the biosciences*, 11(1) 2024, p. lsae001.
   - DOI: https://doi.org/10.1093/jlb/lsae001
3. Brkan, M.: The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. *German Law Journal*, 20(6) 2019, pp. 864-883.
   - DOI: https://doi.org/10.1017/glj.2019.66
4. Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 10 July 2018 – Tietosuojavaltuutettu v Jehovan todistajat – uskonnollinen yhdyskunta (Case C-25/17), 10.07.2018.
5. Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 16 July 2020 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Case C-311/18), 16.07.2020.
6. Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 5 June 2018 – Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (Case C-210/16), 05.06.2018.

7. Court of Justice of the European Union: Judgment of the Court (Grand Chamber) of 4 July 2023 – Meta Platforms Inc. and Others v Bundeskartellamt (Case C-252/21), 04.07.2023.

8. Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 19 October 2016 – Patrick Breyer v Bundesrepublik Deutschland (Case C-582/14), Judgment of 19.10.2016.

9. Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 20 December 2017 – Peter Nowak v Data Protection Commissioner (Case C-434/16), 20.12.2017.

10. Court of Justice of the European Union: Judgment of the Court (Second Chamber) of 29 July 2019 – Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (Case C-40/17), 29.07.2019.

11. Custers, B., Malgieri, G.: Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data. *Computer Law & Security Review*, 45(July) 2022, pp. 1-13.
    - DOI: https://doi.org/10.1016/j.clsr.2022.105683

12. European Data Protection Board: *Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1*, Brussels: European Data Protection Board, 4.5.2020.

13. European Data Protection Board: *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, Brussels: European Data Protection Board, 20.10.2020.

14. European Data Protection Board: *Guidelines 8/2020 on the targeting of social media users*, Brussels: European Data Protection Board, 13.4.2021.

15. European Data Protection Board: *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, Brussels: European Data Protection Board, 17.12.2024.

16. Fedushko, S., Mastykash, O., Syerov, Y., Peráček, T. Model of user data analysis complex for the management of diverse web projects during crises. *Applied Sciences*, 10(24) 2020, pp. 1-12.
    - DOI: https://doi.org/10.3390/app10249122

17. Funta, R., Buttler, D.: The digital economy and legal challenges. *InterEULawEast*, 10(1) 2023, pp. 145-160.
    - DOI: https://doi.org/10.22598/iele.2023.10.1.8

18. Karpiuk, M., Melchior, C., Kaczmarek, K.: A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data. *Prawo i Więź*, 50(3) 2024, pp. 104-121.
    - DOI: https://doi.org/10.36128/PRIW.VI50.907

19. Kesa, A., Kerikmäe, T.: Artificial intelligence and the GDPR: Inevitable nemeses?. *TalTech Journal of European Studies*, 10(3) 2020, pp. 68-90.
    - DOI: https://doi.org/10.1515/bjes-2020-0022

20. Mazurek, G.: Artificial Intelligence, Law, and Ethics. *Krytyka Prawa*, 15(1) 2023, pp. 11-14.
    - DOI: https://doi.org/10.7206/kp.2080-1084.568

21. Mühlhoff, R., Ruschemeier, H.: Updating purpose limitation for AI: a normative approach from law and philosophy. *International Journal of Law and Information Technology,* 33 2025, pp. eaaf003.
    - DOI: https://doi.org/10.1093/ijlit/eaaf003

22. Napieralski, A.: Between the Data Act and the GDPR: Attributing Responsibility for Data Sharing. *Yearbook of Antitrust and Regulatory Studies*, 17(29) 2024, pp. 127-145.
    - DOI: https://doi.org/10.7172/1689-9024.YARS.2024.17.29.4

23. Napieralski, A.: Between the Data Act, the AI Act and the GDPR: purpose limitation and responsibility for secondary data use. *Yearbook of Antitrust and Regulatory Studies*, 18 2025, pp. 101-123.

24. Siwicki, M.: Big Data Profiling and Predictive Analytics from the Perspective of GDPR. *Studia Iuridica Lublinensia*, 32(2) 2023, pp. 249-266.
    - DOI: https://doi.org/10.17951/sil.2023.32.2.249-266

25. Šmejkal, V.: Umělá inteligence jako kvalitativní výzva pro ochranu hospodářské soutěže, in: Mlsna, P. (ed.): *Hospodářská soutěž a veřejné zakázky. Synergie a průsečíky* (pp. 299-318), Plzeň: Aleš Čeněk, 2022.

26. Šramel, B., Horváth, P.: Internet as the communication medium of the 21st century: do we need a special legal regulation of freedom of expression on the internet. *The Lawyer Quarterly*, 11(1) 2021, pp. 141-157.

27. Szuchy, R.: Conformity assessments under the EU AI Act: Ensuring compliance, safety and trust in artificial intelligence. *Legal Business*, 2024, pp. 56-57.

28. Tzanou, M.: Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection. *Croatian Yearbook of European Law & Policy*, 6(1) 2010, pp. 53-74.
    - DOI: https://doi.org/10.3935/cyelp.06.2010.103

29. van der Sloot, B.: Legal fundamentalism: is data protection really a fundamental right?. in: Leenes, R., van Brakel, R., Gutwirth, S., de Hert, P. (eds.): *Data protection and privacy: (in)visibilities and infrastructures* (pp. 3-30), Heidelberg: Springer, 2017.

30. Vardanyan, L., Stehlík, V., Kocharyan, H.: Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity. *TalTech Journal of European Studies*, 12(1) 2022, pp. 159-185.
    - DOI: https://doi.org/10.2478/bjes-2022-0008

31. Wallner, M., Peráček, T.: Data management in industrial companies: the case of Austria. *International Journal for Quality Research*, 17(3) 2023, pp. 847-866.
    - DOI: https://doi.org/10.24874/IJQR17.03-14