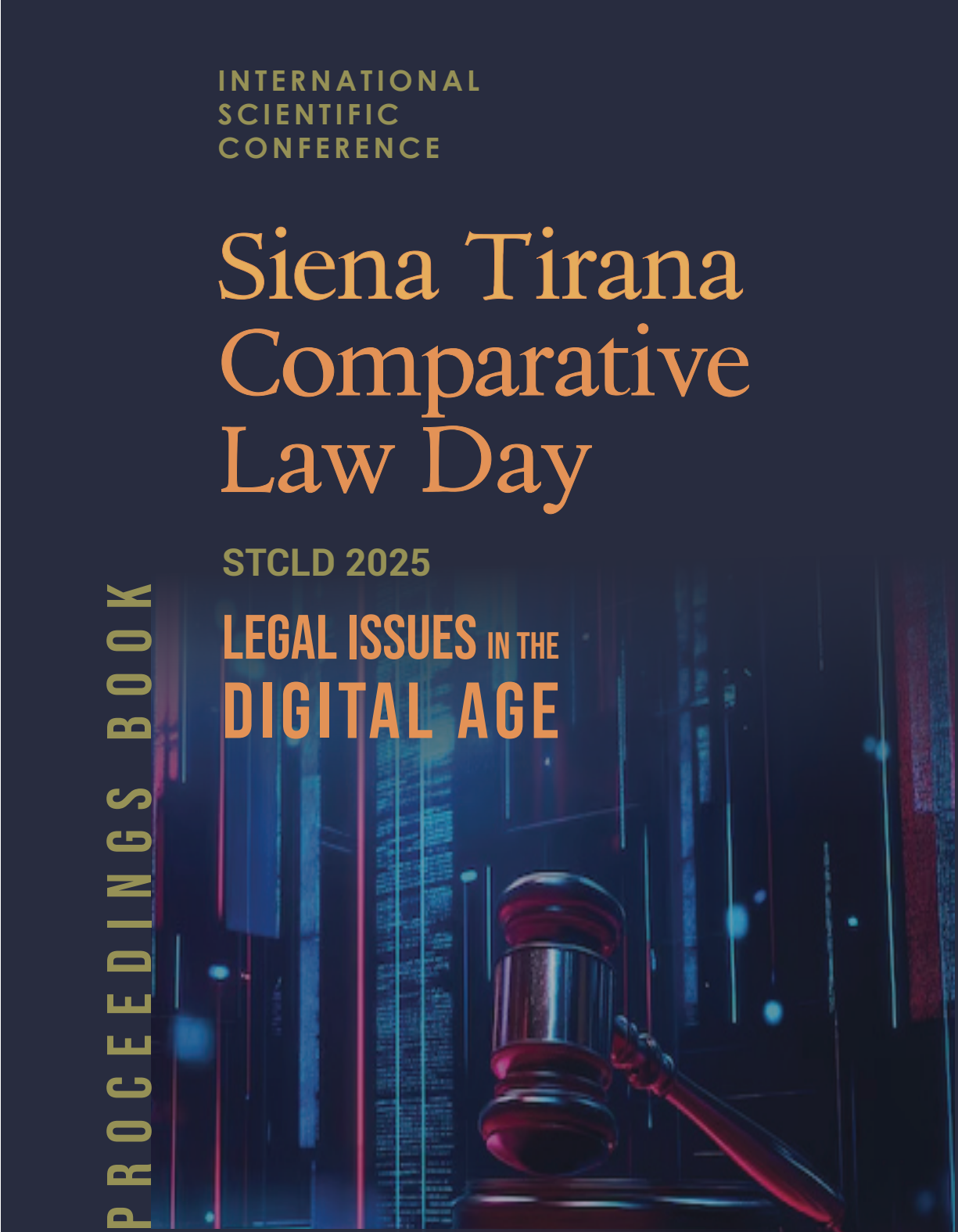
INTERNATIONAL
SCIENTIFIC
CONFERENCE

Siena Tirana Comparative Law Day

STCLD 2025

LEGAL ISSUES IN THE DIGITAL AGE

PROCEEDINGS BOOK



UNIVERSITÀ
DI SIENA
1240

UNIVERSITÀ DI SIENA
1240

DIPARTIMENTO DI GIURISPRUDENZA — DGIUR

UNIVERSITY OF SIENA,
DEPARTMENT OF LAW

UNIVERSITY OF TIRANA, FACULTY OF LAW,
DEPARTMENT OF CIVIL LAW

International Scientific Conference

"Siena-Tirana Comparative Law Day"

Legal Issues in the Digital Age

STCLD 2025

16 May 2025
Siena - Italy

PROCEEDINGS BOOK

Tirana, 2025

UNIVERSITÀ DI SIENA 1240 — DIPARTIMENTO DI GIURISPRUDENZA — DGIUR

UNIVERSITY OF SIENA,
DEPARTMENT OF LAW

UNIVERSITY OF TIRANA, FACULTY OF LAW,
DEPARTMENT OF CIVIL LAW

International Scientific Conference

"Siena-Tirana Comparative Law Day"

Legal Issues in the Digital Age

STCLD 2025

16 May 2025
Siena - Italy

SCIENTIFIC COMMITTEE

Prof. Dr. Artan Hoxha, University of Tirana, Albania
Prof. Dr. Dorina Hoxha, University of Tirana, Albania
Prof. Alessandro Palmieri, University of Siena, Italy
Prof. Dr. Kestrin Katro, University of Tirana, Albania
Prof. Assoc. Renata Tokrri, University of Tirana, Albania
Prof. Valeria Piergigli, University of Siena, Italy
Prof. Giammaria Milani, University of Siena, Italy
Prof. Paolo Guarda, University of Trento, Italy
Prof. Dr. Eriona Katro, University of Tirana, Albania
Prof. Assoc. Anjeza Liçenji, University of Tirana, Albania
Prof. Assoc. Ersida Teliti, University of Tirana, Albania
Prof. Assoc. Artan Saphiu, University of Tirana, Albania
Prof. Assoc. Ilda Melo, University of Tirana, Albania

PROCEEDINGS BOOK

ISBN 9789928826800

Tirana, 2025

The importance of Standard Contractual Clauses in the Data Processing Agreement

Roberta Nucciarone

Abstract

This article examines the crucial role of Standard Contractual Clauses (SCCs) in shaping Data Processing Agreements (DPAs) within the framework of the General Data Protection Regulation (GDPR). It begins by examining the evolving relationship between data controllers and processors, focusing on the contractual obligations established under Article 28 GDPR. Particular attention is given to the formal and substantive requirements that DPAs must fulfill, including liability distribution and compliance mechanisms. The article then analyzes the SCCs adopted by the European Commission and by national data protection authorities, specifically Denmark and Croatia, assessing their effectiveness in addressing regulatory ambiguities. While SCCs serve as important tools for ensuring GDPR compliance and harmonizing data protection practices, the study reveals significant shortcoming, especially regarding the regulation of liability and the risk of imbalance between contracting parties. The Danish model, although pioneering, delegates too much responsibility to the parties themselves, while the Croatian model, despite offering more specific guidance on liability, ultimately refrains from going beyond the wording of the GDPR. In light of these findings, the article argues for a renewed institutional effort to develop more comprehensive and prescriptive SCCs, in order to clarify the more ambiguous aspects of the GDPR and to promote greater fairness and legal certainty in Data Processing Agreements throughout the European Union.

Keywords: *Data Controller, Data Processor Relationship, Data Processing Agreement (DPA), Standard Contractual Clauses (SCCs), Liability*

1. Introduction

Over time, businesses have increasingly acquired the role of crossroads for information flows, finding themselves "processing," as data controllers, a growing number of data belonging to all those individuals who, in various ways, come into contact with the company. To manage such data, companies have turned to

external parties, namely data processors. Before proceeding with the analysis, it is necessary to first clarify the meaning of some key concepts that have already emerged in this initial overview. First of all, the concept of "data processing", which refers to "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means" [1]. These operations include, for example, the collection and storage of data, as well as its use and dissemination. Once the meaning of processing has been explained, it is necessary to identify the parties involved, namely the data controller and the data processor. The term "data controller" refers to the entity that collects the data in order to use it for its own purposes. In fact, what distinguishes the controller is the ability to determine the purposes and means of processing. Instead, the term "data processor" refers to "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"[2]. From this definition, the contrasting role of the processor compared to the controller clearly emerges; while the latter determines the purpose, the former acts in accordance with the predetermined processing purposes. The relationship between the two subjects is, therefore, characterized by the instrumental role of the processor with respect to the controller's interests. In addition to acting on behalf of the controller, the processor must also follow the controller's instructions and submit to their supervision. Indeed, the processor is bound to the controller by a relationship of subordination, a legal relationship through which the appointing party (the controller), with a formal appointment, assigns the processor the managementof the processing of data[3].

Regarding the appointment of the processor, it is governed by GDPR, which states: "processing by a processor shall be governed by a contract or other legal act under Union or Member State law"[4]. In these terms, the GDPR introduces the Data Processing Agreement (DPA), which is the contract through which the data controller appoints a data processor to manage the activities of data collection and processing, imposing both formal and substantive obligations on the parties. Regarding the formal aspect, the GDPR, stipulating that the contract or legal act must necessarily be in written form, including electronic forms, has introduced a formal requirement *ad substantiam*[5].In this sense, it differs from the previous legislation, where the formal obligation was solely *adprobationem*[6]. Furthermore,

[1]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, (General Data Protection Regulation) [2016], OJ L119/1 ('GDPR'), art. 4(1).
[2]GDPR, art. 4(8).
[3]Massimini M., *Il responsabile del trattamento* (2006)<https://privacy.it/archivio/massimini01.html> accessed 8 May 2025.
[4]GDPR, art. 28(3).
[5]GDPR, art. 28 (9).
[6]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995], OJ L281/31 ('DPD'), art. 17(4).

Directive 95/46/EC, in the aforementioned article, only required the processor to comply with the controller's instructions. In contrast, under the GDPR, the European legislator has placed greater emphasis on the content of the Data Processing Agreement, introducing both general and specific provisions.

As for the general provisions, the European legislator requires the contract to regulate "the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the data controller"[7]. However, the most innovative aspect lies in the specific provisions, namely the series of clauses listed under the third paragraph of the article that GDPR mandates the parties to adopt within their DPAs. Among all these obligations, it is important to highlight the requirement for the processor to process data only on the controller's instructions,since the more detailed the controller's instructions are, the easier and more straightforward the allocation of liability between the data processing parties will be.In fact, both the controller and the processor are liable for damages arising from unlawful data processing, with the processor being held liable for damages if they fail to comply with the obligations directly imposed on them by the GDPR or if they act in a manner inconsistent with or contrary to the lawful instructions of the controller[8]. Furthermore, in the event that both parties are liable, the controller and the processor are jointly liable for the full amount of the damage. This liability framework necessitates that the controller's instructions be specified as much as possible within the DPA in order to circumscribe the roles and liabilities clearly.

While it is true that the GDPR requires controllers and processors to be as detailed as possible when drafting the DPA, it is also true that the European legislator has allowed them flexibility in regulating various aspects, including liability. Indeed, this discretion often leads to gaps in the DPAs and potential abuses by the contractually stronger part. If this is true, it must be also emphasized that the legislator provides controllers and processors with support tools, granting supervisory authorities, as well as the European Commission, the authority to issue standard contractual clauses (SCCs) to be used as the DPA[9].

2 - The Standard Contractual Clauses of the European Commission

By virtue of this power, on June 4, 2021, the European institution approved the set of standard contractual clauses that govern the relationship between data controllers and data processors (DPA SCCs)[10]. These clauses represent a model

[7] GDPR, art. 28(3).
[8]GDPR, art. 82 (2).
[9]GDPR, art. 28 (7), (8).
[10]Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[2021], OJ L 199/18, 7.6.2021.

agreement that organizations can use to comply with the GDPR rules related to data processing by controllers and processors. Adoption of the SCCs is not mandatory;in fact,the actors of data processing have four different options for entering into their DPA. The first is to use the standard clauses in their entirety, which can then be considered either as an independent contract or as an addendum to a broader contract, the Master Services Agreement. The second option is to supplement the SCCs, which are fully incorporated into the contract, with additional clauses.The third option is to adopt only part of the clauses, incorporating some into existing agreements. The final option is to ignore the Commission's clauses and create their own models, provided that they include all the provisions required by the GDPR.In light of these alternatives, the most convenient choice for the parties seems to be to include all the SCCs in the agreements, because only in this case the presence of the clauses will ensure compliance with the GDPR standards. If the clauses are partially referenced or fully included in the agreement with modifications to the text, the SCCs would no longer constitute a guarantee of the DPA's compliance with the Regulation. Although controllers and processors cannot amend the standard clauses, they can further specify the obligations set out in the agreement, for example, the data storage locations and the deadline by which the data must be returned to the controller upon termination. The addition of such specifics allows for the alignment of the clauses with internal processes, and it also enables the weaker party to balance the SCCs that may appear more favourable to the other part[11].

Among the aspects not addressed by the European Commission, which therefore deserve further consideration by the processing parties, is the liability of the controllers and processors. Far from dedicating a specific article to it, the Commission only mentions liability between "technical and organizational measures, including technical and organizational measures to ensure data security"[12].

Therefore, although the Institution has acknowledged the need for specific clauses on liability, as it requires that all the measures in the annex be defined in a non-generic manner by the parties, it does not provide them with any input, limiting itself to requiring that the agreement should include, among other things, "measures for ensuring accountability"[13]. This highlights the limitation of standard contractual clauses, which have left crucial aspects of the controller-processor relationship, including the liability under article 82 of the GDPR, to be freely regulated by the parties themselves.

[11]L.Brodahl *et al., EU Commission Publishes Template Data Processing Agreement*(2021)<https://www.wsgrdataadvisor.com/2021/06/eu-commission-publishes-template-data-processing-agreement./>accessed 8 May 2025.
[12]Commission Implementing Decision (EU) 2021/915, annex 3.
[13]Ibidem.

3 - The Standard Contractual Clauses of the Danish Data Protection Authority

Moving on to an example of standard contractual clauses developed by a national data protection authority, it is possible to examine the case of Denmark. In 2018, the Danish Data Protection Authority (Datatilsynet) identified the difficulties faced by national companies in entering into Data Processing Agreements that complied with the minimum requirements of art. 28 of the GDPR. As a result, the Authority exercised the power granted by the Regulation to adopt standard contractual clauses to govern the relationship between controllers and processors. This model was then submitted for review by the European Data Protection Board (EDPB), in accordance with articles 28(8) and 64(1)(d) of the GDPR, which stipulate that a supervisoryauthority may adopt SCCs in line with the consistency mechanism (GDPR, art. 64), involving the EDPB and, where relevant, the European Commission. In July 2019, the European Data Protection Board issued an opinion on the Danish Authority's standard contractual clauses, the first to present SCCs to the EDPB[14]. In light of this opinion, Datatilsynet updated its model and resubmitted it to the EDPB, completing the consultation procedure.

As with the European Commission's standard contractual clauses, it is not mandatory for processing parties to use the Danish Authority's SCCs, provided their DPAs comply with the GDPR requirements. However, using the standard contractual clauses is particularly advantageous for the parties, as it prevents Datatilsynet from conducting a review of the part of the agreement that replicates the SCCs. Regarding the content of the standard contractual clauses, the European Committee has made both general observations on Data Processing Agreements and specific comments on the Danish Authority's model[15]. An example in this regard is the observation made by the EDPB regarding the technical and organizational measures that must be implemented by the processor. In the Committee's view, the model should require the parties to specify which measures[16] are most suitable to assist the data controller, as well as the scope and extent of the required assistance[17]. This approach also applies to other assistance obligations, particularly the obligation for the processor to ensure minimum levels of security by adopting measures that reduce the risk to the rights and freedoms of data subjects[18].All these measures must be fully detailed in an appendix to

[14]European Data Protection Board, *'EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA* (Article 28(8) GDPR) (2019)< https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf>accessed 8 May 2025.

[15]Datatilsynet, *Standardkontraktsbestemmelser vedtaget af Datatilsynet* (2019)<https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/dec/standardkontraktsbestemmelser-vedtaget-af-datatilsynet>accessed 8 May 2025.

[16]GDPR, art. 28, (3)(e).

[17]EDPB Opinion 14/2019, para 3 (2), (9).

[18] GDPR, art. 28, (3) (f).

the SCCs. Furthermore, the EDPB has requested that Datatilsynet integrate provisions related to sub-processors, noting that any clause granting authorization for sub-processing, whether general or specific, should be included in the SCCs or form part of their appendix. Similarly, the list of sub-processors accepted by the controller should be part of the standard contractual clauses. Additionally, the European Committee has expressed the need for a specific clause recognizing the controller's right to oppose changes to sub-processors, which should also establish a sufficient time frame for the exercise of this power[19]. Although the EDPB has made specific observations on many of Datatilsynet's clauses, it did not require any amendments or changes to clause number 13, the only one mentioning the liability of the controller and processor. In fact, this clause allows the parties to regulate aspects of the processing not addressed by any other SCC, including liability. However, it adds nothing regarding the criteria for attributing liability, nor does it address theexoneration evidence or the case of joint liability explicitly provided for by the Regulation. Given the brevity of this clause, one would have expected the Danish Authority to demand more specific provisions, just as it did for the organizational and security measures. On the contrary, the EDPB limited itself to recommending that any additional paragraphs in the agreement, whether concerning liability, jurisdiction, or any other term, do not contradict the relevant provisions of the GDPR or undermine the level of protection offered by the Regulation[20]. In light of these considerations, it emerges that the model of the Danish Authority has indeed benefited local businesses, as they can conclude legally binding agreements when they incorporate the SCCs. However, it is also important to note that Datatilsynet has overlooked crucial aspects of data processing, such as the liability of the controller and processor. In fact, the standard contractual clauses, apart from reiterating the necessary compliance with the GDPR, leave the regulation of liability entirely to the parties. In this way, the Danish model only encourages the inclusion of clauses that disadvantage the weaker part, for example, by stipulating that the weaker part should indemnify the other in case of damage.

Therefore, it is undeniable that Datatilsynet should be considered a model for other supervisory authorities, being the first to activate the Regulation's procedure for the creation of standard contractual clauses; at the same time, there are several aspects that the Danish authority has failed to regulate, leaving the task of managing them to the actors involved in the processing, with all the risks this entails.

[19] EDPB Opinion 14/2019, para 3 (2) (7).

[20] A. Fernandez, *EDPB Opinion 14/2019 on Standard Contractual Clauses for Processors under Article 28(8) GDPR (2019*), 5 (4)*European Data Protection Law Review*523.

4. The Data Processing Agreement model of the Croatian Data Protection Authority

The Danish Data Protection Authority was not the only one to develop a model of Data Processing Agreement usable by national actors of data processing. Although it did not adopt the procedure for standard contractual clauses, the Croatian Data Protection Authority (Agencija za zaštituosobnihpodataka or AZOP), due to increasing inquiries about the necessity of an agreement between the controller and processor, as well as the procedure for concluding this kind of agreement, developed its own model of Data Processing Agreement[21]. The model represents a detailed attempt to align with the requirements set forth by the GDPR. It is meticulously crafted to ensure the effective management of data processing activities, with a strong emphasis on clear delineation of responsibilities and obligations between the controller and the processor.The first crucial element to highlight is the emphasis placed on the definition of the scope and extent of the data processing activities. Furthermore, it is established that the controller and the processor shall define, through the agreement, the obligations they are subject to, as well as the rights they possess, in accordance with data protection regulations. In addition to the subject matter, the model focuses on the types of data processed and the categories of data subjects to whom the data relates, specifying that both must be listed in annex 1[22]. By demanding that controllers and processors explicitly identify the types of personal data and the categories of data subjects, the agreement establishes a clear framework for understanding the boundaries within which data processing can occur. This clause reflects a careful attempt to mitigate ambiguity, which often leads to misinterpretation of processing activities and potential breaches.

Equally important is the model's treatment of the instructions issued by the controller. In accordance with the GDPR, the processor is obligated to act only under the documented instructions of the controller. The model reinforces this, specifying that instructions may be amended or supplemented over time, and they must be provided in written or electronic form. This provision allows for the dynamic nature of data processing activities, particularly in a rapidly evolving digital landscape where new types of processing activities may arise, or regulatory adjustments may necessitate changes in processing practices.Regarding the instructions, the model also introduces a significant safeguard whereby the processor is not only required to comply with the controller's instructions but also has the right to suspend compliance if it believes the instructions are non-

[21]AZOP, *Ugovor o obradi podataka između voditelja obrade i izvršitelja obrade prema članku 28. st. 3.Opće uredbe o zaštiti podataka sklapa se između (*2022) <https://azop.hr/ugovor-o-obradi-osobnih-podataka-izmedu-voditelja-obrade-i-izvrsitelja-obrade-sukladno-odredbama-opce-uredbe-o-zastiti-podataka/>accessed 8 May 2025.
[22]Ibid para 4.

compliant with data protection laws[23]. This clause underscores the liability of the processor to ensure that all processing is GDPR-compliant. In terms of security measures, the model outlines the necessity for the processor to implement both technical and organizational measures as outlined in art. 32 of the GDPR. This includes ensuring that the level of protection is adequate to safeguard the rights and freedoms of data subjects. The DPA model also provides a mechanism for the processor to modify these measures, as long as they do not compromise the level of protection agreed upon with the controller[24].

Additionally, the AZOP has regulated the role of the sub-processor complying with the GDPR (art. 28, para2 and 4): its appointment is conditional upon the written consent of the controller,and it is subject to the same obligations that apply to the processor under the controller-processor agreement. Any replacement or addition of a sub-processor must be communicated to the controller by the processor. However, regarding the controller's right to object to such changes, the model makes a clarification, stating that this right must be exercised within ten days. As for the liability for actions or omissions by the sub-processor that violate the agreement, the model, once again, does not deviate from the Regulation, stating that the processor is liable for such actions[25].

Finally, the agreement focuses on the termination of the main contract, contemplating two different scenarios: extraordinary termination, exercisable by the controller if the processor fails to comply with the obligations arising from the agreement, or seriously violates the Regulation, national data protection laws, and the instructions of the controller[26]; and ordinary termination, under which the processor is required, as with the termination of the agreement, to return or delete all documents and data received from the controller, unless deletion is prohibited by national or Union provisions. Compliance with this obligation can be verified by the controller either personally or by using independent, non-competing experts. However, these are not the only obligations arising from ordinary termination, as the processor, even after the conclusion of the main contract, is required to maintain confidentiality regarding the processed data[27].

In the model agreement just described, AZOP did not fail to regulate the liability of the controller and the processor towards the data subject[28]. Although the Croatian Authority had the opportunity to define in detail what is generally established by the Regulation, in this case it merely refers to article 82 of the GDPR both regarding the joint liability of the controller and processor, and regarding the burden of proof. Indeed, the agreement excludes liability for the party that proves it did not cause the damage to the data subject: in other words, the non-imputability of the harmful event.As for the allocation of liability, the model

[23]Ibid para 5.
[24]Ibid para 6.
[25]Ibid para 9.
[26]Ibid para 12.
[27]Ibid para 13.
[28]Ibid para 11.

stipulates that, if the controller requests it, the processor is obliged to indemnify the controller from any claims for damages from data subjects, provided that these claims arise froma violation of the obligations the processor owes to the controller under the Regulation; actions the processor takes contrary to the instructions of the controller. Even if the indemnification of the controller is subject to an explicit request from this latter, the model does not deviate from the GDPR, which states that "a processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller"[29]. Although the wording of the provision raises some concerns, as it places the liability on the initiative of the controller, which has a foundation in the Regulation and could risk appearing as an indemnity clause[30], it is clear that the model attributes liability to the processor in the same circumstances as the GDPR, namely for failing to comply with its obligations or with the instructions of the controller.

In terms of liability, it should be noted that the AZOP model has provided some additional elements for controllers and processors about to enter into a Data Processing Agreement. At the very least, the Croatian Authority's agreement does not overlook liability; on the contrary, it dedicates a specific section to it, offering, despite all its limitations, guidelines for both the controller and the processor.

5. Conclusion

In light of the analysis just conducted, it cannot be denied that the GDPR was decisive in regulating the controller-processor relationship by providing the obligation for the parties to enter into a DPA. On the other hand, it also emerged that article 28 GDPR, as formulated, has led to various problems, which the European Commission and the national supervisory authorities have been called upon to solve. However, what has been achieved so far by the Commission, as well as by the individual national authorities, seems insufficient to guarantee the dissemination of Data Processing Agreements that truly protect the parties involved. For this to happen, new standard contractual clauses need to be formulated by the European Commission, or in any case by a significant number of national control authorities, which will shed more light on the more obscure aspects of the Regulation.

[29]GDPR, art 82 (2).
[30]T. W. Marriott, *Indemnities in Contracts'*(1956), 11(2) *Industrial Law Review* 110.

Bibliography

AZOP, *Ugovor o obradi podataka između voditelja obrade i izvršitelja obrade prema članku 28. st. 3.Opće uredbe o zaštiti podataka sklapa se između (*2022) <https://azop.hr/ugovor-o-obradi-osobnih-podataka-izmedu-voditelja-obrade-i-izvrsitelja-obrade-sukladno-odredbama-opce-uredbe-o-zastiti-podataka/>accessed 8 May 2025.

Brodahl L. *et al*., *EU Commission Publishes Template Data Processing Agreement* (2021) <https://www.wsgrdataadvisor.com/2021/06/eu-commission-publishes-template-data-processing-agreement./> accessed 8 May 2025.

Datatilsynet, *Standardkontraktsbestemmelser vedtaget af Datatilsynet* (2019) <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/dec/standardkontraktsbestemmelser-vedtaget-af-datatilsynet> accessed 8 May 2025.

European Data Protection Board, '*EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA* (Article 28(8) GDPR) (2019)<https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf> accessed 8 May 2025.

Fernandez A., *EDPB Opinion 14/2019 on Standard Contractual Clauses for Processors under Article 28(8) GDPR (2019)*, 5 (4) *European Data Protection Law Review* 523.

Massimini M., *Il responsabile del trattamento* (2006) <https://privacy.it/archivio/massimini01.html> accessed 8 May 2025.

MarriottT. W., *Indemnities in Contracts'*(1956), 11(2) *Industrial Law Review* 110.

CIP Katalogimi në botim BK Tiranë

Universiteti i Tiranës. Fakulteti i Drejtësisë
Siena-Tirana comparative law day : legal issues in the digital age : STCLD 2025 : proceedings book / University of Tirana, Faculty of Law, Department of Civil Law University of Siena, Department of Law. - Vlorë : Triptik, 2025.
372 f. ; 23 cm.

ISBN 9789928826800

1.Të drejtat civile 2.Baza të të dhënave 3.Mbrojtja 4.Konferenca
347 (062)
004.3 (062)

INTERNATIONAL SCIENTIFIC CONFERENCE

Siena-Tirana Comparative Law Day

LEGAL ISSUES IN THE DIGITAL AGE

STCLD 2025

PROCEEDINGS BOOK