SENTINEL

Bridging the security, privacy, and data protection gap for smaller enterprises in Europe

D2.5 - Continuous data privacy legislation compliance monitoring and guidelines - final version

This work is part of the SENTINEL project. SENTINEL has received funding from the European Union's Horizon 2020 Work Programme for research and innovation 2018-2020 under grant agreement n°101021659.

Project Information

Grant Agreement Number	**101021659**
Project Acronym	SENTINEL
Project Full Title	Bridging the security, privacy, and data protection gap for smaller enterprises in Europe
Starting Date	1st June 2021
Duration	36 months
Call Identifier	H2020-SU-DS-2020
Topic	H2020-SU-DS-2018-2019-2020 Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises
Project Website	https://www.sentinel-project.eu/
Project Coordinator	Dr. George Bravos
Organisation	Information Technology for Market Leadership (ITML)
Email	gebravos@itml.gr

Document Information

Work Package	Work Package 2
Deliverable Title	D2.5 - Continuous data privacy legislation compliance monitoring and guidelines - final version
Version	1.3
Date of Submission	24/11/2023
Main Editor(s)	Prof. Fereniki Panagopoulou (CECL), Dr Tania Kyriakou (CECL)
Contributor(s)	Dimitra Malandraki (CECL)
Reviewer(s)	Marinos Tsantekidis (AEGIS), Eleni-Maria Kalogeraki (FP)

Document Classification							
Draft		Final	X	Confidential		Public	X

History			
Version	**Issue Date**	**Status**	**Distribution**
1.0	01/11/2023	Draft	Confidential
1.1	08/11/2023	Draft ready for review	Confidential
1.2	20/11/2023	Review process completed	Confidential
1.3	24/11/2023	Final after review comments	Public

Table of Contents

Abbreviations

Abbreviation	Explanation
AEPD	Agencia Espaňola de Protección de Datos (Spanish DPA)
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale de l'Informatique et des Libertés (French DPA)
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
EDAC	Ethical & Data privacy Advisory Committee
EDPB	European Data Protection Board
EEA	European Economic Area
GDPR	General Data Protection Regulation
HDPA	Hellenic DPA
ICO	Information Commissioner's Office (UK DPA)
ME	Micro Enterprise
NDA	Non-disclosure agreement
ROPA	Records of Processing Activity
SCCs	Standard Contractual Clauses
SME	Small and Medium-sized Enterprise

Executive Summary

The purpose of this report is to showcase the most significant legal developments concerning the Small and Medium-sized Enterprises/Micro Enterprises (SMEs/MEs) compliance with the General Data Protection Regulation (GDPR) from 1 June 2021 to date in the framework of the SENTINEL project.

The report summarises the most important legal developments concerning SMEs compliance with the GDPR in the light of the EU legislation, the European Data Protection Board's (EDPB's) Directives and Opinions and the Decisions of the National Supervisory Authorities.

This report aims to give the SMEs the opportunity to receive updates on all developments concerning compliance and guidance under the GDPR. Moreover, they can be informed about some GDPR violation cases by some SMEs and the corresponding penalties imposed on them by the National Supervisory Authorities.

At the end of this report, the problems that SMEs seem to face, regarding their effective and practical compliance with the GDPR and how they affect them are exposed, while possible and realistic preventive solutions for SMEs are discussed, reflecting the core objective of the SENTINEL tool.

The report reflects the activities of Task 2.5 and enhances the content of D2.4 with recent decisions and guidelines of supervisory authorities.

1. Introduction

1.1 Purpose of the document

The purpose of this document is to record the continuous monitoring of EU rules and guidelines with respect to privacy and personal data protection, performed by the project's Ethics Supervisor in collaboration with the EDAC. The recorded developments will inform the SENTINEL data protection and privacy compliance framework components and help ensure that all technologies, architectures, frameworks and methodologies are compliant with the evolving landscape of GDPR and other EU regulations. The current report presents the progress of Task 2.5 activities of WP2, which is related to the activities of Task 8.4 of WP8 and enhances the deliverable D2.4 [1] on additional supervisory authorities' decisions of interest for SMEs.

1.2 Structure of the document

The document comprises two main chapters. The first one lists opinions and guidelines issued by the European Data Protection Authority (EDPB) and national Data Protection Authorities (DPAs) within the reference period (1 June 2021 – 31 October 2022). The second chapter illustrates their impact on SMEs and MEs data protection policies. Eventually, the last chapter draws the conclusions of the report.

1.3 Intended readership

This is a public deliverable. The content found in this document aims to help all stakeholders and all interested parties beyond the direct beneficiaries of the project to understand the most important legal developments concerning SMEs' compliance with the GDPR.

1.4 Updates since D2.4

There were no developments in terms of SMEs related EDPB guidelines/ EU legislation since the last version of the deliverable. However, additional supervisory authorities' decisions of interest for SMEs have been added in the respective sections.

2. Analysis – The most significant legal developments concerning the SMEs' compliance with the GDPR

2.1 The EU's ''New Standard Contractual Clauses (SCCs) for cross-border data transfers (June 2021)

On 4th of June 2021 and following the annulment of the Privacy Shield by the CJEU in July 2020, due to the failure of the US to provide a satisfactory and equivalent level of protection to the EU, the European Commission introduced the "New Standard Contractual Clauses (SCCs) [2]", under which transfers of personal data from the EU and the European Economic Area (EEA) to third countries whose data protection regimes have not been assessed by the Commission, would henceforth be carried out. According to the European Data Protection Board (EDPB), in the absence of a Commission adequacy decision, the controller is competent to judge the status of the Member State. The same was ruled by the CJEU in the Schrems II Decision [3].

In the adoption of the New Standard Contractual Clauses, the Schrems II Decision of the CJEU has undoubtedly played an important role, as it seems that the new clauses are adapted to new technological developments and challenges, since data transfers to third countries may on the have an extraterritorial application.

2.2 The EDPB's Opinion 1/2022 on the draft decision of the Luxembourg Supervisory Authority regarding the GDPR-CARPA certification criteria (February 2022)

On 01/02/2022, the EDPB issued an Opinion (1/2022) 0 of major importance for the evolution of data protection concerning the criteria of the certification mechanism introduced by the Luxembourg Supervisory Authority.

In more detail, Luxembourg became the first country in national and international level to introduce a certification mechanism (''GDPR-CARPA'') [3] according to the GDPR criteria. However, before officially adopting the mechanism, the Luxembourg Supervisory Authority submitted the draft decision for the adoption of the GDPR-CARPA certification mechanism to the EDPB.

The EDPB, for the first time, adopted a consistency Opinion concerning the criteria of a national certification mechanism. Moreover, the EDPB's Opinion intended to ensure consistency and sound application of the certification criteria by the Supervisory Authorities of the European Economic Area.

Some of the most important observations made by the EDPB concerning the GDPR-CARPA scheme are the following:

1. According to the EDPB, the GDPR-CARPA certification mechanism is a general mechanism, which does not focus on a specific sector or type of processing, but includes requirements relating to the management of data protection in the organisation surrounding the processing activities.

2. The EDPB noted that the GDPR-CARPA scheme did not mention the exclusion of processing activities falling under Articles 85 to 89 GDPR. Moreover, it did not mention the suitable and specific measures to safeguard the fundamental rights and interests of data subjects required under Article 89(1) of the GDPR. Thus, the EDPB recommended the LU SA to include specific criteria covering processing activities under Articles 85 to 89 of the GDPR [5]. Furthermore, the EDPB recommended the LU SA to include that an analysis of the relevant laws shall be performed by the entity which demonstrates that specific and suitable measures have been put in place, in order to respect the fundamental rights and interests of data subjects pursuant to Article 89 of the GDPR.
3. Moreover, the EDPB recommended the LU SA to amend the certification criteria, in order to provide the factors that shall be taken into account by the applicant when carrying out the relevant assessments, so as to also clarify what will be checked by the certification body.
4. Further, the EDPB recommended the LU SA to make clear that there are processes in place to measure and ensure the effectiveness of the said plan, so as to ensure that the certification criteria are self-explanatory and that the certification body could know what it needs to check from the sole formulation of the criteria.
5. Furthermore, the EDPB encouraged the LU SA to add that the reports on control performed regarding the implementation of organisational and technical measures the draft certification criteria stated, should be provided also to the relevant persons within the organisation who are involved – so not only to the DPO and the entity's management.

According to the EDPB, the GDPR-CARPA certification mechanism is not a certification, according to Article 46(2)(f) of the GDPR, meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in letter (f) of Article 46(2). Indeed, any transfer of personal data to a third country or to an international organisation, shall take place only if the provisions of Chapter V of the GDPR are respected.

To this end, the EDPB considered that certain changes should be made to the draft certification mechanism decision, given that following the approval by the Supervisory Authority, the mechanism should also be added to the register of certification mechanisms and data protection seals, in accordance with the Article 42 par. 8 GDPR.

The most important focal points of the EDPB's Opinion 1/2022 are the following:

1. According to Article 42(1) of the GDPR, Member States, the EDPB and the European Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, **for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors, taking into account the specific needs of micro, small and medium-sized enterprises.**

2. According to Recital 100 of the GDPR, **the establishment of certifications can enhance transparency** and allow data subjects to assess the level of data protection of relevant products and services.
3. The Opinion aims **to ensure the consistent application of the GDPR.**
4. **Certification mechanisms should enable controllers and processors to demonstrate compliance with the GDPR**; therefore, the certification criteria should properly reflect the requirements and principles concerning the protection of personal data laid down in the GDPR and contribute to its consistent application.
5. **The certification criteria should take into account and, where appropriate, be inter-operable with other standards**, such as ISO standards, and certification practices.
6. **Certifications should add value to an organisation by helping to implement standardized and specific organisational and technical measures** that demonstrably facilitate and enhance processing operation compliance, **taking account of sector-specific requirements**.
7. The EDPB welcomes the efforts made by scheme owners to elaborate certification mechanisms, which are **practical and potentially cost-effective tools to ensure greater consistency with the GDPR and foster the right to privacy and data protection of data subjects by increasing transparency**.
8. The EDPB recalls that **certifications are voluntary accountability tools**, and that the adherence to a certification mechanism **does not reduce the responsibility of controllers and processors for compliance with the GDPR or prevent SAs from exercising their tasks and powers pursuant to the GDPR and the relevant national laws**.

2.3 The EU-US Trans-Atlantic Data Privacy Framework Adoption Agreement (March 2022)

On 25 March 2022, the EU and the US agreed in principle, after months of negotiations, on a new framework for transatlantic personal data transfers. The new framework (Trans-Atlantic Data Privacy Framework [6]), will aim to address the issues related to the security of transatlantic personal data transfers, as highlighted by the Schrems II decision of the CJEU in July 2020, as well as to establish "predictability" for transatlantic flows of personal data vital to the economy.

Negotiations on the new mechanism were based on two pillars:

1. The new framework for transatlantic transfers of personal data should meet the requirements set by European standards for the US side to meet the criteria of "necessity" and "proportionality" (which are also the narrow core of the fundamental principle of proportionality in constitutional law) when it comes to US intelligence authorities' access to personal data transferred from the EU for national security activities.

2. The new framework, should provide an adequate and effective redress mechanism for European citizens/residents whose personal data have been unlawfully processed.

In addition, the new framework will provide an enduring basis for transatlantic data flows, which are critical to protect citizens' rights and enhance transatlantic trade. Further, **by enhancing cross-border data flows, the new framework will promote an inclusive digital economy in which everyone can participate and in which businesses of all sizes can thrive.**

Furthermore, the new framework strengthens cooperation between the EU and the US as a wider community of democracies, with the ultimate goal of achieving security, respecting privacy and creating economic opportunities for businesses and citizens. The EU-US Trade and Technology Council and other organisations, such as the Organisation for Economic Co-operation and Development, will also serve these purposes in relation to digital policies.

For the time being, the EU and the US are continuing to work together to translate this agreement into legal documents, which must be approved by both sides in order to implement the Trans-Atlantic Data Protection Framework. To this end, these commitments on the US side will be included in an executive order, which will form the foundation for a future adequacy decision by the European Commission.

2.4 EDPB's Guidelines 07/2022 on certification as a tool for transfers (June 2022)

On 14 June 2022, the EDPB adopted Guidelines 07/2022 [7] regarding certifications as a tool for transfers.

According to the Guidelines, the GDPR requires in its Article 46 that data exporters shall put in place appropriate safeguards for transfers of personal data to third countries or international organisations. To that end, the GDPR diversifies the appropriate safeguards that may be used by data exporters under Article 46 for framing transfers to third countries by introducing, amongst others, certification as a new transfer mechanism (Articles 42 (2) and 46 (2) (f) GDPR). Guidelines 07/2022 provide guidance as to the application of Article 46 (2) (f) of the GDPR on transfers of personal data to third countries or to international organisations on the basis of certification.

In more detail, in the first Part of the Guidelines, the EDPB clarifies that the Guidelines supplement the already existing general Guidelines 1/2018 [8] on certification and addresses specific requirements from Chapter V of the GDPR when certification is used as a transfer tool. According to Article 44 of the GDPR, any transfer of personal data to third countries or international organisations, must meet the conditions of the other provisions of the GDPR in addition to complying with Chapter V of the GDPR. Therefore, as a first step, compliance with the general provisions of the GDPR must be ensured and, as a second step, the provisions of Chapter V of the GDPR must be complied with. The actors who are involved and their core roles in this context are described, with a special focus on the role of the data importer who will be granted a certification and of the data exporter who will use it as a tool to frame its transfers (considering that the responsibility for data processing compliance remains with the data exporter). In this context the certification can also include additional measures that supplement transfer tools to

ensure compliance with the EU level of protection of personal data. Part one of the guidelines also contains information on the process for obtaining a certification to be used as tool for transfers.

Moreover, the second part of the Guidelines recalls that the requirements for accreditation of a certification body are to be found in ISO/IEC 17065 and by interpreting the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the GDPR and its Annex against the background of Chapter V. However, in the context of a transfer, these Guidelines further explain some of the accreditation requirements applicable to the certification body.

The third part of the Guidelines provides for guidance on the certification criteria already listed in Guidelines 1/2018 and establishes additional specific criteria that should be included in a certification mechanism to be used as a tool for transfers to third countries. These criteria cover the assessment of the third country legislation, the general obligations of exporters and importers, rules on onward transfers, redress and enforcement, process and actions for situations in which national legislation and practices prevents compliance with commitments taken as part of certification and requests for data access by third country authorities.

Part four of the Guidelines specifies what should be addressed in the binding and enforceable commitments that controllers or processors not subject to the GDPR should take for the purpose of providing appropriate safeguards to data transferred to third countries. These commitments, which may be set out in different instruments, including contracts, shall, in particular, include a warranty that the importer has no reason to believe that the laws and practices in the third country applicable to the processing at stake (including any requirements to disclose personal data or measures authorising access by public authorities) prevent it from fulfilling its commitments under the certification.

Finally, the ANNEX of the Guidelines contains **some examples** of supplementary measures in line with those listed in Annex II Recommendations 01/2020 [9] (Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data) **in the context of using certification as a tool for transfers**.

2.5 HDPA (Hellenic Data Protection Authority) Decisions

The HDPA, between June 2021 **and today, has issued a series of decisions, whereby fines have been imposed on SMEs for their non**-compliance with the GDPR.

Some of these decisions are as follows:

a) HDPA 29/2021 [10]

The Authority examined a complaint against a controller for **failure to comply with the right of access** exercised by a father on behalf of his minor child in the exercise of parental responsibility. The controller did not comply with the Authority's relevant instruction to satisfy the complainant's right of access to his minor child's personal data, as evidenced by a relevant Authority document. The Authority instructed the controller to provide the requested documents to the complainant. Finally, the Authority **imposed an administrative fine of 3,000 euros on the controller** for

failure to comply with the right of access **and a fine of 5,000 euros for failure to comply with an order of the Authority.**

b) HDPA 37/2021 [11]

The Authority examined a complaint against a data controller **for failure to comply with the right to erasure of a data subject** from a website maintained by the data controller, containing a public directory of doctors. The complainant twice exercised her right to erasure by sending an email to the address provided by the controller as a means of communication on its website but received no response.

The Authority found **a violation of the principle of lawfulness and restriction of processing** under Art. 5(1)(a), (e) and 6(1) of the GDPR by **the unlawful retention and processing of personal data** on the website of the audited company **despite the existence of a legitimate request for erasure.**

Furthermore, the Authority found a **lack of compliance of the company, as a controller, with the provisions of the GDPR** and in particular with regard to the satisfaction of the rights of the data subjects. The Authority issued a compliance order within one month and **imposed an administrative fine 5,000 euros on the controller.**

c) HDPA 48/2021 [12]

A company, which conducts distance selling by telephone, used customers' data collected during the purchase of products to promote its products and services. **This processing constitutes the use of personal data for a purpose other than that for which the data were originally collected**, therefore the criteria of Article 6(4) of the GDPR should be ensured. In this case, it was found that **the data subject was not adequately informed** at the stage of data collection so that he or she was aware that his or her data would be used for a further different purpose, that the objections of the customers were not respected and that the identity of the controller was not clear to the data subjects.

Also, regarding the fulfilment of **the right to object**, the controller did not provide adequate documentation or instructions to demonstrate that it was able to respond to such requests. **The Authority imposed a fine of 20,000 euros for the violations found.**

d) HDPA 56/2021 [13]

The Authority examined nine complaints concerning automated telephone promotions by an advertising company, one complaint against the same company concerning the sending of unclaimed promotional SMS, as well as its general practice regarding its promotional activities.

The Authority found violations of Article 11(1) of Law 3471/2006 (carrying out automated telephone actions **without prior consent** - since, in addition to the fact that the company did not prove that it obtained consents, the very procedure it described as following **did not ensure that valid consents were obtained),** as well as violations of Articles 13 and 14 of the GDPR (**failure to inform the data subjects** - since, inter alia, the complainants did not even initially know the name of the company that made the calls). **The Authority imposed a fine of 30,000 euros for the above-mentioned violations.**

e) HDPA 36/2022 [14]

The Authority, in the course of its examination of a complaint, found that the non-availability of an imaging examination requested by the complainant from a diagnostic centre, constituted a **violation of the principle of Article 5(1)(f) of the GDPR (integrity and confidentiality)**, due to the **failure to take appropriate technical organisational measures** to ensure an appropriate level of security pursuant to Article 32 of the GDPR, and thus **imposed an administrative fine of 30,000 euros on the diagnostic centre.**

In addition, it found that the notification of a personal data breach to the Authority was made late in violation of Article 33 of the GDPR and thus issued a warning pursuant to Article 58(2)(b) of the GDPR to the diagnostic centre. Finally, the Authority issued an order, pursuant to Article 58(2)(e) of the Greek Civil Code, to the Commission for a preliminary investigation, to the diagnostic centre to communicate the personal data breach to the affected data subjects, in accordance with Article 34 of the GDPR.

f) HDPA 50/2022 [15]

The Authority examined the lawfulness of the operation of a video surveillance system in a private educational establishment following a complaint by a former employee.

The evidence submitted showed that the video surveillance system did not fulfil the conditions of lawfulness. Specifically, the Authority during its investigation found that the school did not have a sufficient legal basis for the video surveillance. In view of the extensive video surveillance and the resulting restriction of the personal rights of the data subjects, the school could not rely on a legitimate interest (protection of property). In addition, the Authority found that the controller had violated its duty to inform teachers and parents by notifying them only verbally and incompletely about the video surveillance system.

Moreover, **violations of the Articles 5(1)(a) (lawfulness, fairness and transparency), 5(1)((b) (purpose limitation), 5(2) (principle of accountability) and the Articles 6 (lawfulness of processing), 12 (transparent information), 13 (information to be provided where personal data are collected from the data subject) and 30 (records of processing activities) of the GDPR were found**. Thus, the Authority **imposed an administrative fine of 15,000 euros** on the controller and ordered it to uninstall the cameras and to inform the Authority in writing.

g) HDPA 51/2022 [16]

The Authority examined a complaint concerning the non-fulfilment of the complainant's right of access to a record containing personal data concerning his minor child and, according to a recorded image of a video surveillance system installed in the complainant's private business (gas station). The transmission of the material to the police authorities during the investigation of an incident without informing the subject, was also complained about.

The Authority **imposed a fine of 3,000 euros for violations of the Articles 12 (deadline for informing non-action on right) and 14 (information to be provided where personal data have not been obtained from the data subject) of the GDPR.**

h) HDPA 45/2022 [17]

The Authority examined a complaint by an unemployed person against the Greek labour recruitment agency (OAED) for leaking his personal data and against two educational training and counseling centres (KEK) for the unlawful processing of his data. The complainant, who had registered in the registers of the OAED after expressing his interest in participating in a subsidised employment and training programme of the Ministry of Labour, received a telephone call from the two complained KEKs in order to receive the training services provided by them.

The examination of the complaint did not reveal any instance of data leakage on the part of the OAED. As regards the first KEK, it was found that the complainant, during their initial telephone communication, believed that he was talking to representatives of the OAED, being confused, which was due, at least in part, to the incomplete and unclear information he had received from the OAED. Therefore, the Authority **addressed a warning to the first KEK for the observed failure to comply with the principle of transparency**.

The second KEK complained against, while initially claimed to have found the complainant's details through an internet search, subsequently claimed that the complainant had filled in an expression of interest form on its website, through which he provided his consent, a fact that the complainant denies.

Moreover, it was found that **the consent procedure invoked by the second KEK did not meet the requirements of the Article 7 of the GDPR (conditions for consent) and was not valid, in particular due to incomplete information and the lack of procedures to confirm the data provided**, while in addition, the KEK carried out a further search of the complainant's data on the internet in the context of the examination of the complaint, **without substantiating the lawfulness of the above processing operations, nor the compliance with the principle of transparency towards the complainant**.

For this reason, **a fine of 10,000 euros was imposed** on the second KEK **for violations of the Articles 5(1) (principles relating to the processing of personal data), 6(1)(a) (legal basis of consent), 7 (conditions for consent), 12 (transparent information) and 13 (information to be provided where personal data are collected from the data subject)**.

2.6 CNIL’s (French Data Protection Authority) Decisions

a) Délibération SAN-2021-008 du 14 Juin 2021 [18]

CNIL carried out three inspections between 2018 and 2021 on BRICO PRIVÉ company, which publishes a private sales website dedicated to DIY, gardening and home improvement. This company operates in France and three other European countries (Spain, Italy and Portugal). During its inspections, CNIL found several shortcomings in the processing of personal data of prospective clients and customers. In addition, given that the persons concerned were located in different countries of the European Union, CNIL's Limited Supervisory Committee cooperated, for part of the decision, with the Supervisory Authorities of the three countries in which BRICO PRIVÉ offers its services.

During the inspections, CNIL identified the following violations of the GDPR: **Non-compliance with the obligation to limit the duration of data retention (Article 5(1)(e) of the GDPR), non-**

compliance with the obligation to inform individuals (Article 13 of the GDPR), non-compliance with the obligation to respect the right to erasure (Article 17 of the GDPR) and failure to ensure the security of data processing (Article 32 of the GDPR).

In addition, the following infringements outside the GDPR were also identified: Failure to comply with the obligation to obtain consent from individuals for commercial searches by email (Article L. 34-5 of the CPCE); and violation concerning cookies (Article 82 of the Data Protection Law).

At the end of this procedure, **CNIL imposed a fine of 500,000 euros for violations of the GDPR** and decided to publicise its decision. In addition to the violations of the GDPR, which were the subject of a cooperation procedure with the Spanish, Italian and Portuguese Supervisory Authorities, the sanction imposed concerned violations relating to e-commerce and cookies. Finally, CNIL also required the company to bring its processing procedures into compliance with article L.34-5 of the CPCE and article 5(1)(e) of the GDPR and to justify this within three months of the notification of the decision with a fine of 500 Euro per day of delay.

b) Délibération SAN-2022-015 du 7 Juillet 2022 [19]

In the context of the 2020 priority thematic area on new uses of geolocation data in the context of mobility, CNIL carried out research on a company, which rents vehicles for short periods of time. The investigations focused in particular on the data collected, the retention periods set, the information provided to individuals and the security measures applied by the company.

During the investigations, CNIL found the following violations of the GDPR: **Failure to comply with the obligation to ensure the minimisation of data (Article 5(1)(c) of the GDPR), failure to establish and respect a proportionate data retention period (Article 5(1)(e) of the GDPR – storage limitation) and failure to inform individuals (Article 12 of the GDPR – transparent information).**

On the basis of these findings, **CNIL, in cooperation with the other European Authorities concerned (Belgium, Denmark, Spain, Italy and Germany), imposed a fine of 175,000 Euro** on UBEEQO INTERNATIONAL and decided to publicise its decision.

2.7 AEPD (Spanish Data Protection Authority) Decisions

a) AEPD – PS-00487-2021 [20]

AEPD investigated a company that provides financial services, after a data subject's complaint.

During the investigation, AEPD found that the controller **had no legal basis for processing the data and violated the Article 6(1) of the GDPR.**

Therefore, **the AEPD fined the controller 40,000 Euros, that were reduced to 24,000 Euros due to acknowledgement of responsibility and early payment.**

b) AEPD – PS-00105-2022 [21]

AEPD audited a company that organises road running races.

During the investigation, AEPD found that **the controller did not have an effective legal basis for processing health data and violated the Articles 6 and 9 of the GDPR.**

Thus, **AEPD imposed a fine of 16,000 Euros on the company that was reduced to 9,600 Euros due to voluntary payment and admission of responsibility.**

c) AEPD – PS-00246-2022 [22]

AEPD investigated a magazine company – producer of children's educational magazines and found that unauthorized persons had accessed the company's database and thus unauthorizedly siphoned off location and contact data of users of the database. Approximately *470,000 users* were affected by the incident. The DPA's investigation determined that a vulnerability in the controller's systems allowed the incident to occur.

During the investigation, **AEPD found the following violations of the GDPR: Violation of the Article 32 GDPR (security of the processing) and violation of the Article 33 GDPR (notification of a personal data breach to the Supervisory Authority).**

AEPD fined the controller 52,000 euros for all the violations combined. This was reduced to 31,200 Euros, because the controller had already paid part of the fine voluntarily, in the context of the controller's admission of guilt.

d) AEPD – PS-00097-2022 [23]

AEPD investigated the controller of a company who had entered personal data of an employee in the Social Security General Employee Register without the employee ever having actually worked. For this reason, the controller would have been obliged to cancel the entry of the data subject in the register within 72 hours, which the controller failed to do. In the absence of the data subject's work performance, the controller **no longer had a legal basis** to upload the data to the register.

Therefore, AEPD found that the failure to delete the data constituted **an unlawful processing of the data subject's personal data** and thus **imposed a fine of 5.000 euros on the company for the violation of the Article 6 (1) (lawfulness of processing).**

e) AEPD – PS-00310-2022 [24]

AEPD investigated a complaint of an individual regarding a restaurant's controller who obliged clients to fill out a form with their personal information for contact tracing purposes in the context of the Covid-19 pandemic.

However, during its investigation, the DPA found that the legal basis for collecting the contact information had expired, in the meantime, and the controller had therefore processed the data unlawfully.

AEPD also found that the controller did not provide data subjects with sufficient information on data processing. Moreover, AEPD determined that the controller did not provide data subjects with an easy way to object to the processing of personal data.

Thus, AEPD imposed a fine of 3,600 euros on the restaurant for the violation of the Articles 6(1) (lawfulness of processing), 13 (information to be provided where personal data are collected from the data subject) and 21 (right to object) of the GDPR.

f) AEPD – PS-00158-2022 [25]

AEPD investigated a media and editorial company since several media outlets, including the controller had published an audio recording of a multiple rape victim's testimony in court on their websites. The case had attracted a lot of media attention.

During its investigation, AEPD determined that the rape victim's **right to privacy outweighed the controller's freedom of information.**

The audio recordings of the victim did not add significant value to the reporting but rather **severely compromised the victim's privacy.**

For this reason, and for the **violation of the Article 5(1)(c) (data minimization) of the GDPR**, AEPD **imposed a fine of 50,000 euros** on the company.

g) AEPD – PS-00200-2023 [26]

AEPD investigated a complaint by an individual against a building services company due to the fact that the company had published a picture of the complainant without prior permission.

Moreover, the claimant stated that the picture the company published on its website was the same that motivated the imposition of 1,200 euros fine in the procedure **PS-00346-2022** in 2022 and that the company had again committed the same infraction.

After its investigation, AEPD **initially imposed a fine 2,000 euros on the company for the violation of the Article 6(1) (lawfulness of processing) of the GDPR** that **was reduced to 1,200 euros** due to voluntary payment and admission of responsibility.

h) AEPD – PS-00633-2022 [27]

AEPD investigated a complaint against a cosmetic surgery clinic. The complainant stated that she had received an e-mail by the clinic, including the e-mail addresses of 21 recipients, as the e-mail was sent without using the "blind copy" option.

After its investigation, AEPD imposed **a fine of 1,500 euros** on the clinic **for the violation of the Articles 5(1)(f) (integrity and confidentiality) and 32 (security of the processing) of the GDPR.**

2.8 ICO's (UK's Information Commissioner's Office) Decisions

a) ICO – Mermaids – MPN (2021) [28]

ICO investigated the transgender charity Mermaids, after a data breach report from the charity.

During the investigation, ICO found the following violations of the UK GDPR: Violation of the Article 5(1)(f) (integrity and confidentiality) and violation of the Article 32(1), (2) (security of processing).

Thus, ICO fined the charity 29,000 euros for failing to protect the personal data of its users.

b) ICO – Tuckers Solicitor LLP – MPN (2022) [29]

ICO investigated the law firm Tuckers Solicitors following a ransomware attack on its systems. The attackers managed to encrypt files that contained both personal and special category data, such as medical records, witness statements, names and addresses of witnesses and victims, and the alleged crimes of data subjects, and publish them in underground data marketplaces. As part of its investigation, **ICO determined that Tuckers had failed to take appropriate technical and organizational measures to protect personal data. This failure left its systems vulnerable to malicious attacks.**

Moreover, during the investigation, **ICO found violations of the Articles 5(1)(f) (integrity and confidentiality), 32(1)(a), and 32(1)(b) of the GDPR (security of processing).**

Therefore, **ICO fined law firm Tuckers Solicitors LLP 115,000 Euros.**

3. The impact on SMEs, the solution, and the objective

3.1 Synopsis

In accordance with all the above, the following is observed:

In general, the adoption of the new SCCs by the EU for secure cross-border data transfers, as a result of the annulment of the Privacy Shield, is a major institutional development regarding cross-border data transfers law.

Furthermore, also relevant to cross-border data transfers is the recent EU-US agreement to adopt the New Trans-Atlantic Data Protection Framework, expected to be implemented as a foundation for a future adequacy decision.

At the level of guidelines on compliance with the GDPR, **the EDPB's Opinion 1/2022 on the draft decision of the Luxembourg Supervisory Authority is of great importance, as it highlights a new perspective on the compliance of SMEs, through the establishment of certification mechanisms by national Supervisory Authorities**· in addition, in order for an SME to be certified, specific criteria need to be met, which will be provided for by the mechanism concerned.

However, the EDPB identified some deficiencies in the draft decision concerning the content of the criteria and their practical application when an SME is under assessment, and how they should be applied, e.g., the adoption of technical and organisational measures and whatever else the applicant should take into account when carrying out assessments.

3.2 The impact of the EDPB’s Opinion 1/2022 on SMEs

To summarise, what SMEs must retain from the Opinion 1/2022 is the following:

- It seems very important and helpful for SMEs that they shall have the opportunity to certify that the processors processing data for them are in compliance with the GDPR through certification mechanisms approved by EU national Supervisory Authorities, which will take into account the specific needs of SMEs.
- The establishment of certification mechanisms shall enhance transparency, but also the right to privacy and data protection.
- Certification mechanisms will enable controllers and processors to demonstrate compliance with the GDPR.
- Certifications shall add value to an SME, by helping to implement standardised and specific organisational and technical measures that demonstrably facilitate and enhance data processing compliance, taking account of sector-specific requirements.
- The certification mechanisms are considered practical and potentially cost-effective tools that ensure greater consistency with the GDPR.

- Nevertheless, certifications are voluntary accountability tools· therefore, the adherence to a certification mechanism does not reduce the responsibility of controllers and processors for compliance with the GDPR or prevent them from exercising their tasks and powers pursuant to the GDPR and the relevant national laws.

3.3 The impact of the national Supervisory Authorities' Decisions on SMEs

As we can conclude from the Decisions of national Supervisory Authorities concerning violations of the GDPR by SMEs, the practical and effective compliance and implementation of the GDPR is a pressing problem for SMEs.

In the attempt to crystallise the problem, it appears that the complaints submitted against SMEs mainly concern:

- The violation of the principles relating to the processing of personal data (Article 5 GDPR)
- The violation of the lawfulness of processing (Article 6 GDPR)
- The violation of the GDPR rules defining the responsibilities and obligations of controllers and processors (Articles 24-31 GDPR)
- The violation of the GDPR fundamental principle of accountability concerning the data controllers (Article 5(2) GDPR)
- The violation and the non-fulfilment of the subjects' rights (Articles 12-22 GDPR)
- The risk of the security of processing (Article 32 GDPR) through the data controllers' failure to take appropriate technical and organisational measures, the non-notification or late notification of the data breach to the Supervisory Authority and the non-communication of a data breach to the data subjects.

3.4 The SENTINEL solution and the objective

As discussed above, the failure of some SMEs to comply properly, practically and effectively with the GDPR is a real and undeniable problem, reflected by the fines imposed by national Supervisory Authorities.

Consequently, the compliance of SMEs should be structured as follows:

1. Appropriate technical and organisational measures should be undertaken by the data controllers, in order to protect the subjects' data
2. Data protection by design and by default should be implemented by data controllers.
3. Data controllers should keep records of the processing activities

4. Processors should cooperate with national Supervisory Authorities
5. Impact assessments should be carried out for the data processing.

Moreover, SMEs may seek the help of smart toolkits, to guarantee their compliance with the GDPR. Thus, SMEs will not be at risk of being reported for GDPR violations or getting fined by the supervisory authorities.

A smart tool through which the SMEs shall implement all the above and achieve full compliance with the GDPR at a cost-effective level is **SENTINEL*.***

In detail, the General Data Protection Regulation (GDPR) establishes rights to individuals regarding the handling of their personal data. However, such rights "***suffer from the absence of technical tools and standards that make the exercise of their rights simple and not overly burdensome***". To underline this statement, the Commission focuses on the right to data portability, which has "practical limitation". Thus, a key-activity is "exploring and enhancing the portability right for individuals under Article 20 of the GDPR, giving them more control over who can access and use machine-generated data". These considerations have provided the vision for SENTINEL's IdMS as a practical and ethical way for SMEs/MEs to manage and process personal information in a GDPR-compliant manner, EU-wide.

Further, a key-aspect of GDPR Compliance, as defined in Article 5(2) of the GDPR is the accountability. Being accountable, aims to demonstrate compliance to three entities: Data subjects, data protection authorities and business partners. Accountability, according to the Opinion 3/2010 (on the principle of accountability) of the Article 29 Data Protection Working Party, "would focus on two main elements: (***i) the need for a controller to take appropriate and effective measures to implement data protection principles; (ii) the need to demonstrate upon request that appropriate and effective measures have been undertaken. Thus, the controller shall provide evidence of (i) above***". By integrating accountability as a principle, GDPR states that the controller, and not the Data Protection Authorities, must demonstrate that the entity is compliant with data protection principles. Thus, **SENTINEL's envisioned GDPR compliance and data protection impact assessment framework should demonstrate SMEs' accountability regarding handling of personal data.**

Furthermore, currently, GDPR compliance assessment toolkits rely heavily on manual activities. In addition, only assessment experts – assessors – are authorised to use these tools. Progress beyond the state-of-the-art, is seen by **SENTINEL** partners as the efficient digital transformation of these toolkits to enable participant organisations to autonomously both self-assess accountability and self-determine privacy and data protection risks for GDPR compliance.

Finally, the SMEs that will choose to use the **SENTINEL** tool will be assured that they will have achieved full compliance with the GDPR. Thus, they will be able to proceed, if desired, to be certified by a certification mechanism approved by a national Supervisory Authority, with the certainty that they will achieve to meet the compliance conditions the respective mechanism will provide in its criteria.

Conclusions

The purpose of this report was to highlight the most important developments concerning the compliance of SMEs/MEs with the GDPR, from June 2021 to the time of this report: i) institutional developments, important guidelines and Opinions of the EDPB were analysed, ii) a number of decisions of the Greek, French, Spanish and British Supervisory Authorities concerning SMEs, which imposed non-negligible fines for violation of the GDPR, were discussed.

As it appears that there is still a lack of compliance or incomplete compliance with the GDPR, SMEs should search for safer, more effective, and holistic ways to comply with the GDPR. The Sentinel tool can provide the SMEs with the security and efficiency they lack.

This vision will be realised by integrating tried-and-tested security and privacy technologies into a unified digital architecture and then applying disruptive Intelligence for Compliance. Combined with a focused methodology for application and knowledge sharing and a wide-reaching plan for experimentation for innovation within SMEs, **SENTINEL *will help SMEs feel considerably more secure and safeguard their customers' assets.*** Further, **SENTINEL*'s hybrid agent-based orchestration and enforcement engine*** operates in a semi-automated way to help SMEs get the required technical and operational measures on-board with minimal human intervention, including for education, training, the implementation and validation of checklists and every other necessary measure to achieve the prescribed data protection resilience and GDPR compliance.

Moreover, **SENTINEL** is **a truly cost-effective solution for SMEs, which requires the holistic digital transformation of existing GDPR compliance toolsets, incorporating gamification and cutting-edge user experience technologies, to allow SMEs to efficiently self-assess accountability and self-determine privacy and data protection risks.**

In this vein, once the SMEs manage to be secure, they could request from certification bodies and national Supervisory Authorities (the existence of which is encouraged by GDPR) to investigate whether they are subject to receive certification.

Consequently, the **SENTINEL** tool, that targets SMEs' end-users and not only assessors, **will enhance the GDPR compliance preparedness level of SMEs by offering an end-to-end digital GDPR & data protection compliance and impact assessment framework** based on the established process assessment principles and well-defined standards. **In this way, subjects' rights will be fully respected and protected, and SMEs will be able to achieve the desirable compliance security, a safeguard, that will keep them out of risks and fines and undoubtedly add business value to them, contribute to their business prosperity, health, and progress.**

References

[1] Deliverable D2.4 (2022), "Continuous data privacy legislation compliance monitoring and guidelines report – Interim version", SENTINEL EU H2020 Project.

[2] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council,

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0914

[3] Case C-311/18, Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, https://curia.europa.eu/juris/liste.jsf?num=C-311/18

[4] EDPB, Opinion 1/2022 on the draft decision of the Luxembourg Supervisory Authority regarding the GDPR – CARPA certification criteria,

https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-12022-draft-decision-luxembourg_en

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[6] European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework of 25 March 2022,

https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087

[7] Guidelines 07/2022 on certification as a tool for transfers, Adopted on 14 June 2022,

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-072022-certification-tool-transfers_en

[8] European Data Protection Board, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, Adopted on 25 May 2018,

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2018/guidelines-12018-certification-and-identifying_en

[9] European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021,

https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

Decisions of the European Data Protection Authorities

[10] HDPA 29/2021

https://www.dpa.gr/el/enimerwtiko/prakseisArxis/mi-ikanopoiisi-dikaiomatos-prosbasis-patera-se-dedomena-anilikoy-teknoy

[11] HDPA 37/2021

https://www.dpa.gr/el/enimerwtiko/prakseisArxis/mi-ikanopoiisi-dikaiomatos-diagrafis-kai-paranomi-diatirisi-kai

[12] HDPA 48/2021

https://www.dpa.gr/el/enimerwtiko/prakseisArxis/mi-nomimi-hrisi-stoiheion-pelaton-gia-proothitiko-skopo-kai-mi

[13] HDPA 56/2021

https://www.dpa.gr/el/enimerwtiko/prakseisArxis/aytomatopoiimenes-proothitikes-tilefonikes-energeies-apo-tin-etaireia

[14] HDPA 36/2022

https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-prostimoy-gia-ti-mi-lipsi-katallilon-tehnikon-organotikon-metron

[15] HDPA 50/2022

https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-dioikitikoy-prostimoy-gia-leitoyrgia-systimatos-binteoepitirisis

[16] HDPA 51/2022

https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-prostimoy-gia-mi-ikanopoiisi-dikaiomatos-prosbasis-se-yliko

[17] HDPA 45/2022

https://www.dpa.gr/el/enimerwtiko/prakseisArxis/prostimo-kai-proeidopoiisi-se-kentra-epaggelmatikis-katartisis-gia

[18] CNIL, Délibération SAN-2021-008 du 14 Juin 2021

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000043668709/

[19] CNIL, Délibération SAN-2022-015 du 7 Juillet 2022

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046070924

[20] AEPD – PS-00487-2021

https://www.aepd.es/documento/ps-00487-2021.pdf

[21] AEPD – PS-00105-2022

https://www.aepd.es/documento/ps-00105-2022.pdf

[22] AEPD – PS-00246-2022

https://www.aepd.es/documento/ps-00246-2022.pdf

[23] AEPD – PS-00097-2022

https://www.aepd.es/documento/ps-00097-2022.pdf

[24] AEPD – PS-00310-2022

https://www.aepd.es/documento/ps-00310-2022.pdf

[25] AEPD – PS-00158-2022

https://www.aepd.es/documento/ps-00158-2022.pdf

[26] AEPD – PS-00200-2023

https://www.aepd.es/documento/ps-00200-2023.pdf

[27] AEPD – PS-00633-2022

https://www.aepd.es/documento/ps-00633-2022.pdf

[28] ICO – Mermaids – MPN (2021)

https://ico.org.uk/media/action-weve-taken/mpns/2620171/mermaids-mpn-20210705.pdf

[29] ICO – Tuckers Solicitor LLP – MPN (2022)

https://ico.org.uk/media/action-weve-taken/mpns/4019746/tuckers-mpn-20220228.pdf

Literature Sources

- Jasmontaitė-Zaniewicz L., Calvi A., Nagy R., Barnard-Wills D., (2021). The GDPR Made Simple(R) For SMEs, VUBPRESS.
- Kuner C., Bygrave L., Docksey C., Drechsler L., (2020). The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press.
- Schünemann W. J., Baumann M., Privacy, (2017). Data Protection and Cybersecurity in Europe, Springer.
- Van Alsenoy B., (2019). Data Protection Law in the EU: Roles, Responsibilities and Liability', Intersentia.
- Voigt P., Von dem Bussche A., (2017). EU General Data Protection Regulation (GDPR), Springer.
- ''Data protection in the EU'', in https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

- “15 things all small businesses need to know about data protection”, ICO in https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/15-things-all-small-businesses-need-to-know-about-data-protection/
- “GDPR-compliant services for businesses” (2019) in GDPR.EU, https://gdpr.eu/compliant-services/ Guidance Note: GDPR Guidance for SMEs, An Coimisiún um Chosaint Sonraí, https://www.dataprotection.ie/en/dpc-guidance/guidance-smes