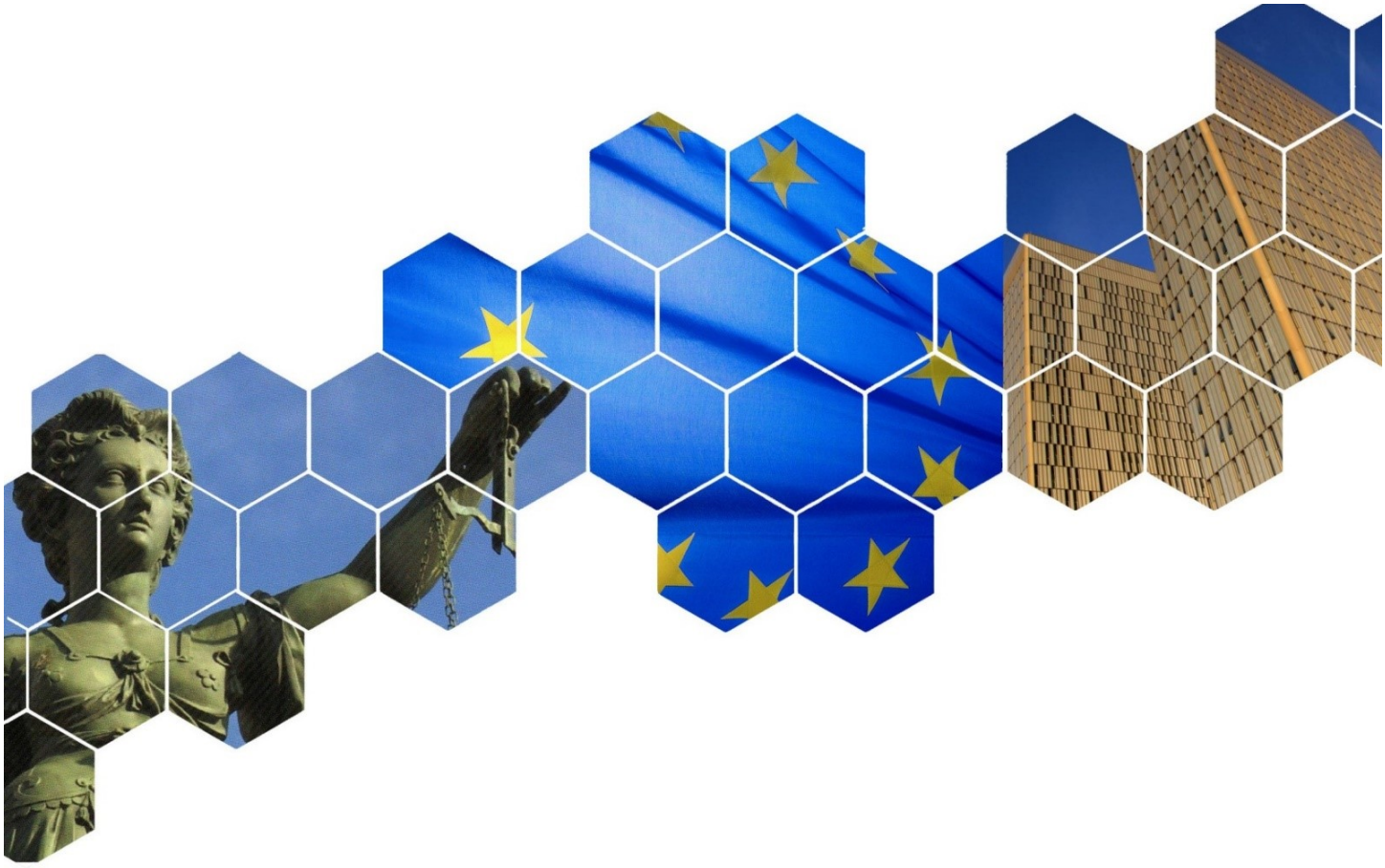
Study on the enforcement of GDPR obligations against entities established outside the EEA but falling under Article 3(2) GDPR

Final Report

Specific contract No. 2020-1103 (EDPS/2019/02-09)



November 2021

This study has been prepared by Milieu under Contract No 2020-1103 (EDPS/2019/02-09) for the benefit of the EDPB.

The study has been carried out by researchers of the Centre de recherche, Information, Droit et Société (CRIDS) at University of Namur (Belgium), with the support of researchers from Milieu Consulting SRL. The leading author of the study report is Jean Herveg (CRIDS).

Milieu Consulting SRL, Chaussée de Charleroi 112, B-1060 Brussels, tel.: +32 2 506 1000; e-mail: EDPB.legalstudies@milieu.be; web address: www.milieu.be.

TABLE OF CONTENT

EXECUTIVE SUMMARY

This Study analyses the possibilities available to enforce Supervisory Authorities' (SAs) investigative and corrective powers against third-country controllers or processors that fall under the scope of Article 3(2) of the General Data Protection Regulation (GDPR), but are not willing to cooperate and did not designate a representative in the European Economic Area (EEA) or the European Union (EU). The analysis focuses on controllers and processors established in California (United States of America, US) and in the United Kingdom (UK). Where possible, the Study provides information on the possibility to enforce these powers against those controllers and processors established in the People's Republic of China (China).

Two main research methods were used: desk research (review of legal literature, national, European and international legal instruments and case-law) and collection of information through a questionnaire sent to the SAs.

The main findings are as follows.

1. Possibility to summon a third-country controller/processor to appear before the SA's Office or its county court

There are some differences between SAs' powers to summon a third-country controller/processor to appear before the SA's Office or in a Court of the SA's country. They are uncertainties as to the possibility for SAs to initiate legal proceedings in another EU Member States or in a third country on the basis of Article 58(5) of the GDPR. The Court of Justice of the European Union (CJEU) case-law is unclear as to whether it could accept to recognise the jurisdiction of a Member State on the basis of Article 58(5) of the GDPR when the controller/processor has no establishment on the territory of any EU Member State.

2. Analysis of the enforcement of SAs' investigative and correctives powers in California, the UK and in China

SAs do not qualify as 'courts or tribunals' in the meaning of Article 267 of the Treaty on the Functioning of the European Union (TFEU) when exercising their investigative and corrective powers and SAs should be considered as exercising 'public powers' under European law when making use of special powers that go beyond those arising from the ordinary legal rules applicable to relationships between private individuals. With respect to this, the wording of Article 58 GDPR might be slightly misleading in respect of the nature of these powers (e.g. Article 58(1) c, e & f) (e.g. 58(2) a, b, c, d, e & g GDPR). If SAs are considered as exercising 'public powers as understood under EU law, there is a possibility that SAs could be considered as acting like 'private persons' in 'civil and commercial matters' (e.g. in the field of international jurisdiction and applicable law).

In theory, SAs may exercise their investigative and corrective powers in a manner that produces effects beyond the EEA territories within the framework of the relevant international law. However, that does not necessarily imply that:

- third countries will accept that SAs exercise investigative and corrective powers in a manner that produces effects on their territories;
- third countries will accept that SAs initiate legal actions or proceedings before their courts or tribunals;
- third countries will recognise that SAs are acting in 'civil or commercial matters' or that they are exercising 'public powers';
- the rules applied by SAs in exercising their investigative and corrective powers are 'acceptable' or 'applicable' in the third countries' courts or tribunals;

- SAs are allowed to send agents abroad to third countries, even with the consent of the controllers/processors established in those countries.

Enforcement of EU SAs' decisions in courts in California and the UK may prove difficult - if not impossible - in a reasonable timeframe without prejudice to its financial cost. However, the adoption of the California Consumer Privacy Act of 2018 may open the door to active cooperation with the California Privacy Protection Agency. Similarly, cooperation with the UK Data Protection Commissioner seems possible in the context of Treaty 108+ (Articles 16 and 17), combined with the functions and missions vested in the UK Commissioner by the UK GDPR and Data Protection Act (DPA 2018). It is worth noticing that the UK Commissioner has concluded a relatively high number of Memorandum of Understanding (MoUs) with foreign data protection authorities. Cooperation with China seems possible in theory but would require a comprehensive approach, including close cooperation with the EU and the Member State public authorities responsible for that relationship with China.

3. Identification of legal instruments supporting the enforcement of SAs' powers

SAs identified legal instruments that could support the enforcement of the GDPR against third-country controllers and processors. The Study highlights some additional instruments that could usefully be considered.

4. Sharing SA experiences and identification of other types of actions

SAs have gained some informal experience of international cooperation. They have identified some avenues to improve international cooperation in the field of data protection, with direct action on the electronic communications infrastructure, or the intermediaries located on the EEA territories appearing most effective (e.g. order to stop collecting personal data or order to shut down a website).

5. Analysis of the possibility to rely on unilateral commitments from controllers/processors on the matters of choice of jurisdiction and applicable law

It appears quite difficult to rely on unilateral commitments from controllers and processors in respect of the choice of jurisdiction or applicable law. However, if SAs are considered to act in 'civil and commercial matters', that opens the way for discussions on the possibility of some degree of choice of jurisdiction and applicable law.

6. Analysis of added value of the designation of controller/processors representatives in the enforcement of SAs' investigative and corrective powers

The appointment of a controller/processor representative is a crucial point for the enforcement of SA investigative and corrective powers.

7. Main obstacles to international cooperation in the field of data protection

SAs have identified several obstacles to international cooperation in the field of data protection, such as lack of practice, shortcomings in the legal framework, problems in producing evidence.

In conclusion, strengthening international cooperation seems to be the best avenue for better and easier enforcement of SAs' investigative and corrective powers against third-country controllers or processors that fall under the scope of Article 3(2) of the GDPR but who are not willing to cooperate with SAs and did not designate an EEA representative. In the short term, the conclusion of MoU (or equivalent) should be considered. The use of legal instruments in the matter of criminal cooperation (such as the Mutual Legal Assistance Treaty (MLAT) concluded with the US) could be considered where there is a serious breach of the GDPR that amounts to a criminal offence. Finally, closer cooperation with the European

Commission when negotiating trade agreements could be useful in considering effective mechanisms to enforce SA investigative and corrective powers abroad.

1 INTRODUCTION

This is the Final Report for the study on 'The enforcement of GDPR obligations against entities established outside the EEA but falling under Article 3(2) GDPR' (the Study), prepared by CRIDS with the support of Milieu, under Specific Contract No Specific Contract No. 2020-1103 (EDPS/2019/02-09) for the European Data Protection Board (EDPB).

1.1 RESEARCH QUESTIONS AND SCOPE OF THE STUDY

Article 3(2) of the GDPR provides that:

> *'This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
> *(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
> *(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.'*

The Study analyses the practical and effective possibilities available to enforce Supervisory Authorities' (SAs) investigative and corrective powers (as set out in Article 58(1) and (2) of the GDPR[1]) against third-country controllers or processors that fall under the scope of Article 3(2) of the GDPR, but are not willing to cooperate with SAs and did not designate a European Economic Area (EEA) Representative.

The Study is limited to controllers and processors located in the State of California (United States of America, US) and in the United Kingdom of Great Britain and Northern Ireland (UK). Where possible, the study provides information on the situation in the People's Republic of China (China). The Study is not limited to the analysis of the GDPR enforcement from the perspective of the five EEA countries mentioned in the Terms of Reference (ToR) (France, Germany, Poland, Spain and Sweden), but, rather, considers inputs received from all the SAs that responded to the questionnaire.

In the context of the Study, a first distinction should be made between:

- the possibility to summon controllers/processors to appear before the SA's Office or in a Court in the SA's country;
- the possibility for the SAs to enforce their investigative and corrective powers against controllers/processors.

The Study does not consider the broader discussion of the possibility for European legislation to produce extra-territorial effects, nor does it contain a theoretical analysis of the issues at stake. That means that the Study left open the numerous and difficult theoretical discussions which can be associated with its subject matter. This analysis is prepared without prejudice to the impact of the circumstances of each real case related to the enforcement of GDPR obligations against entities established outside the EEA.

1.2 METHODOLOGY

Two research methods were used in the Study:

- **Desk work**: desk research, entailing the thorough revision of legislation, international instruments, literature and case-law was completed prior to drafting a questionnaire for the

[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, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1–88.

SAs. The findings of the desk research were also used to structure the main project deliverables and guide the analysis provided in this Final Report. The desk research also entailed the revision of information received from the EDPB, the European Data Protection Supervisor (EDPS) and the European Commission in respect of national mechanisms and international agreements/treaties/mechanisms on the matter of enforcing the GDPR outside the EEA (including provisions that could exist in international trade agreements/treaties);

- **Questionnaire to SAs**: based on the desk research, a questionnaire was designed to collect information from all SAs on the enforcement of the GDPR obligations against entities established outside the EEA but falling under Article 3(2) of the GDPR (identification of specific legal mechanisms and issues, etc.). Sixteen SAs responded (BG, HR, CZ, DK, EE, FI, FR, HU, IS, IT, LT, LU, PL, SK, SI, SE). However, the Study would have benefitted from receiving answers from more SAs.

The Study comprised a series of logical methodological steps, as outlined in Box 1.

Box 1: Methodological steps in completing the Study

(1) Questionnaire:
- Drafting the questionnaire
- Validation of the questionnaire by the EDPB/EDPS
- Dissemination of the questionnaire to national SAs
- Completion of the questionnaire by national SAs

(2) Desk research:
- Compilation and analysis of the outcomes of the questionnaire
- Legal characterisation of the powers conferred on SAs by Article 58 GDPR
- Analysis of international instruments that could impact GDPR enforcement
- Analysis of binding corporate rules (BCR) and standard contractual clauses that could impact GDPR enforcement
- Analysis of the interaction between international public law and GDPR enforcement
- Analysis of the function of a representative (Article 27) and its relationship to GDPR enforcement
- Analysis of international cooperation (Article 50)

(3) Report drafting:
- Legal analysis and first draft of the Report
- Final version of the Report

(4) Quality assurance, editing and validation:
- Quality assurance by senior reviewer and editing
- Interim Meeting with the Client

(5) Finalisation:
- Delivery of the Final Report Draft
- Commenting period for client
- Addressing comments and finalising report
- Final meeting
- Delivery of the Final Report

1.3 REPORT OUTLINE

This report is structured in three sections. Section 1 presents the background, scope and methodology, Section 2 analyses the various aspects of enforcing SAs' investigative and corrective powers, and Section 3 describes the main conclusions of the Study.

Annex 1 contains the template questionnaire used to collect information at EU and national level, Annex 2 lists the sources referenced in the Study, and Annex 3 presents the acronyms and abbreviations used.

2 LEGAL ANALYSIS

Section 2 provides a legal analysis of the following aspects:

- Possibility to summon third-country controllers/processors established in California or in the UK before SAs' Office or in a Court of the SA's country (Section 2.1);
- Analysis of the enforcement of SAs' investigative and correctives powers in California, the UK, and China (Section 2.2);
- Identification of the legal instruments that could support the enforcement of the GDPR against controllers/processors established in a third country (Section 2.3);
- Sharing SAs' experiences and identifying other types of actions (Section 2.4);
- Analysis of the possibility to rely on unilateral commitment from controllers/processors established outside the EEA on matters of choice of jurisdiction and applicable law (Section 2.5);
- Analysis of added value of controller/processor representatives in respect of enforcement of SA investigative and corrective powers (Section 2.6);
- International cooperation foreseen in the GDPR (Section 2.7).

2.1 POSSIBILITY TO SUMMON A THIRD-COUNTRY CONTROLLER/PROCESSOR

Section 2.1.1 outlines whether or not SAs have the legal possibility to summon third-country controllers/processors, as per their questionnaire responses.

Section 2.1.2, analyses whether or not third-country controllers/processors falling under the scope of Article 3(2) of the GDPR could be summoned in cases where they are not willing to cooperate with SAs and did not designate an EEA representative to appear before the SA's Office or in a Court of the SA's country.

Section 2.1.3 outlines a possible outstanding issue even were the right of SAs to summon third-country controllers/processors established in California and the UK to be solved.

2.1.1 Summary of SA responses

The SAs responses showed some uncertainties about the scope of the issue. Some specified possibilities of summoning a controller to appear before a court, others focused on summoning to the SA itself in the course of its administrative proceeding, and still others referenced reporting crimes to the public prosecutor. The same is true of bringing infringements to the attention of the judicial authorities, which may be understood as initiating a civil proceeding in order to defend data subjects' subjective personal rights (e.g. by a judicial order addressed to the controller to refrain from intervening into data subjects' rights to privacy and personality) or reporting crimes to criminal authorities (judicial included). Both understandings have different legal purposes and lead to different answers.

In Bulgaria, the SA has the legal possibility to summon a controller/processor to appear before a court (Article 10 a(2) point 1 of the Bulgarian Personal Data Protection Act (PDPA)). Only Bulgarian law will be applied.

In Czechia, if a person is summoned and fails to appear before an administrative authority without providing an appropriate explanation, the authority can impose a procedural fine of up to CZK 50,000 (EUR 1,956 EUR). A fine may be imposed more than once (Section 62(1,3) of the Administrative Procedure Code). The power to bring infringements of the GDPR to the attention of judicial authorities or to commence or otherwise engage in legal proceedings has not been implemented, however.

In Finland, the national legislation does not include specific data protection rules on the possibility to

summon a controller/processor to appear before a court. According to the Data Protection Act (1050/2018) Section 22 (Conditional fine):

> *'The Data Protection Ombudsman may impose a conditional fine for the purpose of enforcing an order referred to in points (c)–(g) and (j) of Article 58(2) of the Data Protection Regulation and to enforce an order to provide information that has been issued under section 18, subsection 1 of this Act. Provisions on the imposition of a conditional fine and the ordering of its payment are laid down in the Act on Conditional Fines (1113/1990).*
> *No conditional fine shall be imposed on a natural person for the purpose of enforcing an order to provide information referred to in subsection 1 if there are grounds to suspect the person of a criminal offence and the information concerns the matter underlying the suspicion of a criminal offence.'*

However, the Finnish SA has yet to apply Section 22 in practice.

In France, the SA (*Commission nationale de l'informatique et des libertés,* CNIL) has the power to sanction a data controller falling under the scope of Article 3(2) of the GDPR. In that case, the CNIL will pronounce an administrative sanction. The difficulty here lies in enforcement of this decision abroad. A solution is to transfer breaches to the Criminal Court, whose decisions can be enforced in third countries, and GDPR breaches are, in fact, also criminal offences under French law. The French courts will apply the French data protection law. Processing is not qualified as 'cross-border processing' if the data controller has no establishment within the EU, even if personal data of data subjects in the Union are processed by that data controller. The GDPR applies but is not cross-border processing subject to mandatory cooperation between European SAs.

In Croatia, Article 38 of the Act on the Implementation of the General Data Protection Regulation sets out that if, during supervision, knowledge is gained or objects are found that indicate a criminal offence has been committed that could be prosecuted *ex officio*, the authorised persons shall, within the shortest time possible, inform the competent police station or a state attorney. It is unclear whether the SA may summon a controller/processor before the court or to its Office.

In Hungary, Section 2 (5) b) of the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (DPA Act) prescribes the following:

> *'Where personal data are processed within the meaning of the General Data Protection Regulation, the provisions of this Act specified in Subsection (2), and other regulations provided for by law laying down conditions for the protection of personal data and for the processing of personal data shall apply - save where an act or binding legislation of the European Union provides otherwise - if:*
> *(...)*
> *b) the main establishment provided for in Point 16 of Article 4 of the General Data Protection Regulation of the data controller, or the single establishment of the data controller in the European Union is not located in Hungary, however, the processing operations carried out by the controller or processor acting on the controller's behalf or following the controller's instructions, are related to ba) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in Hungary, or bb) the monitoring of the data subjects' behaviour as far as their behaviour takes place within the territory of Hungary.'*

In Iceland, the SA does not have the power to summon a processor/controller to appear before the SA's Office or a court.

In Italy, the Italian SA has the power to summon a processor/controller to appear before the SA's Office or a court (for the latter, see: Article 154-b of the Italian Data Protection Code). The Italian SA considers

that Articles 77, 78 and 79 of the GDPR are the legal bases for the application of the GDPR, also *vis-à-vis* an Article 3(2) controller/processor. The laws will be the same as those applied to a controller/processor under Article 3(1) of the GDPR. Apart from the GDPR rules, Section 166, paragraph 7, of the Data Protection Code, Law No 689/1981 relating to the application of administrative fines (in particular Sections 1-9, 18-22, 24-28) should be applied. Where necessary, Law No 241/1990 on Administrative Procedure and the Right of Access to Administrative Documents and the relevant Italian Freedom of Information Act provisions (Section 5 and 5-a of Legislative Decree No 33 of 2013) could also be applied.

In Lithuania, pursuant to Article 12(2)(9) of the Republic of Lithuania Law on Legal Protection of Personal Data ('the Law'), the SA has the right to receive oral and written explanations from legal and natural persons during the investigation of violations and to demand that they come to the premises of the State Data Protection Inspectorate (SDPI) to give explanations. Pursuant to Article 12(2)(7) of the Law, the SDPI has the right to take part in court proceedings in cases of violations of international, EU and national law provisions on the protection of personal data.

In Luxembourg, no specific procedure is foreseen in national law to allow the SA to directly sue a controller/processor before the courts in relation to Article 58(5) GDPR.

In Poland, in cases of claims for infringements of data protection provisions that can only be asserted in court proceedings, the President of the Polish SA may bring actions in favour of the data subject, with their consent (Article 98(1) of the Act of 10 May 2018 on Personal Data Protection). In such cases, the Act of 17 November 1964, Code of Civil Procedure (Journal of Laws of 2020, item 1575, 1578 and 2320; Journal of Laws of 2021, item 11) is applied.

In Slovenia, the SA does not have the power to summon a processor/controller to appear before the SA's Office or a court.

2.1.2 Consequences of Case C-645/19 on the interpretation of Article 58(5) of the GDPR

In case C-645/19[2] (§§ 78-79), the CJEU ruled that the exercise of Article 58(5) of the GDPR by an SA is not subject to the condition that the controller/processor be established on the territory of the SA's Member State:

> '*It must be observed that Article 58(5) of Regulation 2016/679 is worded in general terms and that the EU legislature has not specified that the exercise of that power by a Member State's supervisory authority is subject to the condition that its legal action should be brought against a controller who has a "main establishment", within the meaning of Article 4, point 16, of that regulation, or another establishment on the territory of that Member State'.*

In addition to this point, the CJEU has limited the consequence of its previous consideration to the condition that the SA's power falls within the territorial scope of the GDPR (with reference to Article 3(1), but also to Article 3(2) and (3) of the GDPR) (Id., §§ 80-84):

> *'80. However, a Member State's supervisory authority may exercise the power conferred on it by Article 58(5) of Regulation 2016/679 only if it is demonstrated that that power falls within the territorial scope of that regulation.*
>
> *81. Article 3(1) of Regulation 2016/679, which governs the territorial scope of that regulation, provides, in that regard, that the regulation applies to the processing of personal*

[2] Case C-645/19: Request for a preliminary ruling from the *Hof van beroep te Brussel* (Belgium) lodged on 30 August 2019 — Facebook Ireland Limited, Facebook Inc., Facebook Belgium BVBA v *Gegevensbeschermingsautoriteit*, OJ C 406, 2.12.2019.

data in the context of the activities of an establishment of a controller or a processor in the European Union, whether or not the processing takes place in the European Union.

82. In that connection, recital 22 of Regulation 2016/679 states that the existence of such an establishment implies the effective and real exercise of activity through stable arrangements and that the legal form of such arrangements, whether through a branch or a subsidiary with legal personality, is not the determining factor in that respect.

83. It follows that, in accordance with Article 3(1) of Regulation 2016/679, the territorial scope of that regulation is determined, without prejudice to the situations referred to in paragraphs 2 and 3 of that article, by the condition that the controller or the processor with respect to the cross-border processing has an establishment in the European Union.

84. Consequently the answer to the second question referred is that Article 58(5) of Regulation 2016/679 must be interpreted as meaning that, in the event of cross-border data processing, it is not a prerequisite for the exercise of the power of a supervisory authority of a Member State, other than the lead supervisory authority, to initiate or engage in legal proceedings, within the meaning of that provision, that the controller with respect to the cross-border processing of personal data against whom such proceedings are brought has a main establishment or another establishment on the territory of that Member State.'

The CJEU also stressed the link between Article 58(5) of the GDPR and the exercise of SAs' powers on their national territory, irrespective of the Member State in which the controller/processor is established (Id., §§ 88-91 & 96):

'88. As regards the power of a supervisory authority of a Member State to bring legal proceedings, within the meaning of Article 58(5) of Regulation 2016/679, it must be recalled, as the Advocate General stated in point 150 of his Opinion, that that provision is worded in general terms and that it does not specify against which entities the supervisory authorities should or might direct legal proceedings in relation to any infringement of that regulation.

89. Consequently, that provision does not restrict the exercise of the power to initiate or engage in legal proceedings in such a way that those proceedings can solely be brought against a "main establishment" or against some other "establishment" of the controller. On the contrary, under Article 58(5) of that regulation, where the supervisory authority of a Member State has the necessary competence for that purpose, under Articles 55 and 56 of Regulation 2016/679, it may exercise the powers conferred by that regulation on its national territory, irrespective of the Member State in which the controller or its processor is established.

90. However, the exercise of the power conferred on each supervisory authority in Article 58(5) of Regulation 2016/679 presupposes that that regulation is applicable. In that regard, and as stated in paragraph 81 of the present judgment, Article 3(1) of that regulation provides that it is applicable to the processing of personal data 'in the context of the activities of an establishment of a controller or a processor in the [European] Union, whether or not the processing takes place in the [European] Union'.

91. Having regard to the objective pursued by Regulation 2016/679, which is to ensure effective protection of the freedoms and fundamental rights of individuals, in particular, their right to protection of privacy and the protection of personal data, the condition that the processing of personal data must be carried out "in the context of the activities" of the establishment concerned, cannot be interpreted restrictively (see, by analogy, judgment of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, paragraph 56 and the case-law cited).

> *96. (...) the power of a supervisory authority of a Member State, other than the lead supervisory authority, to bring any alleged infringement of that regulation to the attention of a court of that Member State and, where appropriate, to initiate or engage in legal proceedings, within the meaning of that provision, may be exercised both with respect to the main establishment of the controller which is located in that authority's own Member State and with respect to another establishment of that controller, provided that the object of the legal proceedings is a processing of data carried out in the context of the activities of that establishment and that that authority is competent to exercise that power, in accordance with the terms of the answer to the first question referred.'*

The CJEU confirmed that Article 58(5) of the GDPR has direct effect, '(…) *with the result that a national supervisory authority may rely on that provision in order to bring or continue a legal action against private parties, even where that provision has not been specifically implemented in the legislation of the Member State concerned* (…)' (Id., §§ 111 & 113):

> '(…) *Article 58(5) of Regulation 2016/679 lays down a specific and directly applicable rule which states that the supervisory authorities must have legal standing before the national courts and must have the power to initiate or engage in legal proceedings under national law*.'

The Court added that there was no need for specific implementation in national law (Id., §§ 111 & 113):

> '(…) *Article 58(5) of Regulation 2016/679 must be interpreted as meaning that that provision has direct effect, with the result that a national supervisory authority may rely on that provision in order to bring or continue a legal action against private parties, even where that provision has not been specifically implemented in the legislation of the Member State concerned*.'

Those questions being settled, it remains to understand whether this judgment could be relied on in assessing whether Article 58(5) GDPR may also be used by SAs against a third-country controller/processor that falls under the scope of Article 3(2) GDPR but is not willing to cooperate with SAs and did not designate an EEA representative to appear in a court in their Member States.

The CJEU appeared to consider Article 58(5) of the GDPR available to SAs as soon as the GDPR applies to the controller, i.e. when the processing of personal data falls under the territorial scope of the GDPR (Article 3), including its application in the situations considered in Article 3(2)-(3).

However, the CJEU also seemed to hold that SAs must exercise their powers on their national territory. It is not clear whether this precludes SAs from initiating legal proceedings in another Member State or in a third country on the basis of Article 58(5) of the GDPR.

The position of the CJEU in respect of the possibility to open any 'international jurisdiction or competence' to the benefit of any 'court or tribunal' of the Member State of the SA on basis of Article 58(5) of the GDPR in cases where the controller/processor lacks any kind of establishment on the territory of any of the Member States, is also unclear.

One possible interpretation is that SAs should be recognised as having the power to summon a third-country controller/processor that falls under the scope of Article 3(2) of the GDPR but is not willing to cooperate with SAs and did not designate an EEA representative to appear in court in their Member State, based on Article 58(5) of the GDPR, for at least four reasons:

- Controller/processor is subject to the GDPR in its totality. There is no formal reason to exclude Article 58(5) of the GDPR;
- As judged by the CJEU, 'the condition that the processing of personal data must be carried out "in the context of the activities" of the establishment concerned, cannot be interpreted restrictively';

- There might be no possibility to initiate any legal proceeding against the controller/processor in the country where it is located or established (for reasons relating to the interpretation of Article 58(5) of the GDPR by the CJEU, or for reasons stemming from the third country's legal rules);
- It could lead to an unexpected competitive distortion between EU-based and non-EU-based controllers/processors.

On the other hand, it should not be disputed that SAs are entitled to summon a third-country controller/processor that falls under the scope of Article 3(2) of the GDPR, but is not willing to cooperate with SAs and did not designate an EEA representative to appear before its Office, based on the provisions of their national law implementing the GDPR.

2.1.3 Key findings

There are differences between SAs' powers to summon third-country controllers/processors to appear before the SA's Office or in a Court of the SA's country. There are uncertainties as to the possibility for SAs to initiate legal proceedings in another EU Member States or in a third country on the basis of Article 58(5) of the GDPR. The CJEU case-law is unclear as to whether it could accept to recognise the jurisdiction of a Member State on the basis of Article 58(5) of the GDPR when the controller/processor has no establishment on the territory of any EU Member State.

If the option to summon a controller/processor that falls under the scope of Article 3(2) of the GDPR but is not willing to cooperate with SAs and did not designate an EEA representative before the SA's Office or a court is initiated, the question of the enforcement of the decision remains, where that controller/processor is uncooperative or does not comply with the court's decision or order.

2.2 ANALYSIS OF ENFORCEMENT OF SAS' INVESTIGATIVE AND CORRECTIVE POWERS IN CALIFORNIA, THE UK AND CHINA

Section 2.2.1 provides a brief analysis of the nature of SAs' investigative and corrective powers.

Section 2.2.2 outlines the possibility for SAs to exercise their investigative and corrective powers beyond the EEA territories.

Section 2.2.3 describes SAs' investigative and corrective powers in California against third-country controllers or processors that fall under the scope of Article 3(2) of the GDPR but are unwilling to cooperate with SAs and did not designate an EEA representative.

Section 2.2.4 outlines SAs' investigative and corrective powers in the UK against third-country controllers or processors that fall under the scope of Article 3(2) of the GDPR but are unwilling to cooperate with SAs and did not designate an EEA representative.

Section 2.2.5 describes SAs' investigative and corrective powers in China against third-country controllers or processors that fall under the scope of Article 3(2) of the GDPR but are unwilling to cooperate with SAs and did not designate an EEA representative.

2.2.1 First preliminary remark: The nature of SAs' investigative and corrective powers

When considering the enforcement of the SAs' investigative and corrective powers against a third-country controller/processor established in California, the UK or China, that falls under the scope of Article 3(2) of the GDPR but is not willing to cooperate with SAs and did not designate an EEA representative, the first issue to analyse is the nature of the SAs' powers.

First, we could think that the nature of SAs' powers should be assessed under the national legislation of the SA's Member State. However, this approach would overlook the fact that SAs now have their legal

basis, status and regime under the GDPR, which is a piece of European legislation (cf. C-645/19, §44).

The issue of determining the nature of the SAs' investigative and corrective powers should therefore be analysed under EU law, with national law characteristics examined only where prescribed or authorised by the GDPR (e.g. Article 58(1)f of the GDPR) or when it is compatible with the GDPR and EU law (including CJEU case-law of the CJEU).

An analysis of all aspects of this (very broad) topic would go beyond the scope of this Study and require far more elaboration (e.g. do SAs qualify as 'European administrative' 'bodies' or 'agencies' or as 'European administrative authorities'). Rather, the Study focuses on two specific aspects that are of interest in the analysis of the nature of SAs' investigative and corrective powers:

- Could SAs qualify as 'courts or tribunals' in the meaning of Article 267 TFEU[3] when exercising their investigative and corrective powers?
- Could SAs be considered to exercise 'public powers' when exercising their investigative and corrective powers?

2.2.1.1 The notion of 'court or tribunal' in the meaning of Article 267 of the TFEU

According to the case-law of the CJEU (e.g. Case VQ v Land Hessen[4], §43), in order to determine whether a body is a 'court or tribunal' within the meaning of Article 267 of the TFEU, the CJEU considers several factors, such as whether:

- the body is established by law;
- the body is permanent;
- the body's jurisdiction is compulsory;
- the body's procedure is *inter partes*;
- the body applies rules of law;
- whether the body is independent.

In this Study it is argued that there is no dispute over the fact that SAs do not qualify as 'courts or tribunals' in the meaning of Article 267 of the TFEU while exercising their investigative and corrective powers. This derives from the interpretation of Article 78 of the GDPR, for example, which provides each natural or legal person with the right to an effective judicial remedy against a legally binding decision of an SA concerning them. If SAs were to be qualified as 'courts or tribunal', this provision would lack meaning[5].

2.2.1.2 The notion of the exercise of 'public powers' in CJEU case-law

While it could easily be concluded that SAs do not qualify as 'courts or tribunals' in the meaning of Article 267 of the TFEU while exercising their investigative and corrective powers, it is less straightforward to assess whether in doing so they exercise 'public powers'.

The case-law of the CJEU (notably in the field of consumer law) may provide some elements to determine whether SAs are exercising 'public powers' (e.g. *Case Belgische Staat v Movic BV*, Events Belgium BV, Leisure Tickets & Activities International BV[6]). The main elements to consider are:

[3] Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, pp. 47–390.
[4] Judgment of the Court (Third Chamber) of 9 July 2020, VQ v Land Hessen VQ v Land Hessen.
[5] See: EDPS, *Data protection in the judiciary: the concept of courts/judicial authorities acting in their judicial capacities*, EDPS/2019/02-01, July 2020.
[6] CJEU, 16 July 2020, *Belgische Staat v Movic BV*, Events Belgium BV, Leisure Tickets & Activities International BV, C-73/19.

'In order to ensure, as far as possible, that the rights and obligations which derive from Regulation No 1215/2012 for the Member States and the persons to whom it applies are equal and uniform, the concept of "civil and commercial matters" of that regulation should not be interpreted as a mere reference to the internal law of a Member State. That concept must be regarded as an autonomous concept to be interpreted by reference, first, to the objectives and scheme of that regulation and, second, to the general principles which stem from the corpus of the national legal systems (Id., §33).'

'Although certain actions where the opposing parties are a public authority and a person governed by private law may come within the scope of Regulation No 1215/2012, it is otherwise where the public authority is acting in the exercise of its public powers (Id., §35).'

'The exercise of public powers by one of the parties to the action, because it exercises powers falling outside the scope of the ordinary legal rules applicable to relationships between private individuals, excludes such an action from "civil and commercial matters" within the meaning of Regulation No 1215/2012 (Id., §36).'

'It follows that, in order to determine whether or not a matter falls within the scope of the concept of "civil and commercial matters" within the meaning of Regulation No 1215/2012, and, consequently, whether it comes within the scope of that regulation, it is necessary to determine (Id., §37):

- *the nature of the legal relationships between the parties to the action and the subject matter of the action;*
- *or, alternatively, the basis of the action and the detailed rules applicable to it*.'

'Actions aimed at determining and stopping unfair commercial practices, within the meaning of Directive 2005/29, are also "civil and commercial matters" within the meaning of Article 1(1) of Regulation No 1215/2012 (Id., §42).'

'The fact that a power was introduced by legislation is not, in itself, decisive in order to conclude that a State authority acted in the exercise of public powers (Id., §47).'

'It follows that the procedural position of the Belgian authorities is, in that regard, comparable to that of a consumer protection association (Id., §49).'

'Acting in the general interest should not be confused with the exercise of public powers (Id., §53).'

'Only where, due to the use to which a public authority has put certain pieces of evidence, it is not specifically in the same position as a person governed by private law in the context of a similar action, would it be appropriate to make a finding that such an authority has, in the particular case, exercised public powers (Id., §57).'

'It should be pointed out that merely collecting and compiling complaints or evidence, as a trade or consumer association could do, cannot amount to the exercise of such powers (Id., §58).'

*'However, as regards the application made by the Belgian authorities to the referring court that it should be granted the power to determine future infringements simply by means of a report issued, on oath, by an official of the Directorate-General for Economic Inspection, such an application cannot be said to come within the scope of 'civil and commercial matters', as that application relates in actual fact to special powers that go beyond those arising from the ordinary legal rules applicable to relationships between private individual*s (Id., §62).'

Deriving from the above, it is understood that SAs could be considered to exercise 'public powers' under EU law when making use of special powers that go beyond those arising from the ordinary legal rules applicable to relationships between private individuals, such as the power to:

- oblige controllers/processors to appear before their Offices;
- inflict fines;
- issue enforceable orders;
- exercise coercive means or methods;
- impose coercive measures;
- act in the capacity of judicial officer;
- draw up authentic statement or report ('on oath'), etc.

It could also be necessary to consider:

- the nature of the legal relationships between the parties to the action and the subject matter of the action; or
- the basis of the action and the detailed rules applicable to it.

It seems certain that the mere existence of investigative powers conferred by law is not enough to characterise the exercise of 'public powers'. In other words, SAs must exercise some kind of 'coercive powers'[7] without prejudice to considering (to some extent) the characteristics of the specific powers that might have been conferred upon them by their national law.

With respect to the exercise of 'public powers' as understood in the CJEU case-law, the wording of Article 58 of the GDPR might be slightly misleading in respect of the nature of some investigative powers (e.g. Article 58(1)c, e, f of the GDPR) and even some corrective powers (e.g. Article 58(2)a, b, c, d, e, g of the GDPR). As a consequence, the very nature of these powers should have to be additionally ascertained in light of the powers conferred on SAs by their national data protection laws: do the latter provide SAs with exorbitant powers that are distinct from those recognised to data subjects or not-for-profit bodies, organisations or associations referred to in Article 80(1) of the GDPR? This will have to be analysed on a case-by-case basis.

2.2.2 Second preliminary remark: The possibility to exercise SAs' investigative and corrective powers beyond the EEA territories

As Freyria already wrote in the 1960s about the potential extra-territorial effects of public law:

> '*It is traditional to assert that public law is territorial. The proposal is flawed by its absolutism and imprecision. Despite its territoriality, social security law follows nationals abroad. A French person who has suffered an accident at work will benefit from the pensions despite his departure abroad. He will receive his old-age insurance pension there as long as he has paid his contributions within the regulatory time limits. In the same way, our tax law imposes a general tax on the French source income received by the French person who leaves to reside abroad. (...) In all these cases, there is no coincidence of our legislation with the geographical framework of our territory. Research must continue well beyond such a primary and superficial formula.* (…)'[8].

In 2018, Azzi recalled that investigation cannot be perform on a foreign territory:

[7] Idot, L., 'La matière civile et commerciale' à l'épreuve de l'intervention du Ministre de l'Economie en droit de la consommation, note sous CJUE (1e ch.), 16 Juillet 2020, aff. C-73/19, *Revue critique de droit international privé*, Paris, Dalloz, 2021/2, p. 383 & s., esp. p. 394, n° 15.
[8] Freyria, Ch., 'La notion de conflit de lois en droit public', in *Travaux du Comité français de droit international privé*, 1962-1964, pp. 106-107.

'*Under international law, it is prohibited for a state to perform an act on foreign territory when it falls within the exclusive competence of the foreign state officials, such as investigation. The consent of the foreign state must be obtained, regardless of the consent of the parties. This rule is shared by every country, including China which codified it under Article 277 of CiPL"*[9].

She added that:

'*Some authors mention the possibility of resorting to international cooperation agreement, such as agreement of mutual legal assistance (MLA). Currently, the vast majority of those treaties are related to criminal cases'*[10].

'*Regarding data protection, some punctual authorisations have been given. It happened for the first time in 1996, when the German DPA obtained the consent of Citibank to conduct an on-site audit of the data processing facilities of its US subsidiary, which had received the credit card data of German customers. A further example is given by the Spanish DPA, which also conducted an audit on the processing equipment of a data recipient in Colombia, on the basis of a contractual clause authorising such an investigation'*[11].

'*These cases raise the question as to whether the cooperation could actually be organised through contractual clauses. Actually, some standard contractual clauses for data transfers outside the EU already contain a prior authorisation given to the relevant DPA. However, as noted by Christopher Kuner, the consent of the relevant government authorities will always be required and, according to him, was obtained by the German and Spanish DPAs in the cases mentioned'*[12].

'*An EU DPA may also overcome the reluctance to consent of the foreign authorities by asking its DPA to conduct the measures itself, on behalf of the EU DPA, but an agreement would have to be reached as to the costs incurred by the operation*'[13].

On the one hand, in case C-18/18, the CJEU judged that Directive 2000/31/EU[14] does not preclude national courts from issuing orders that could produce effects beyond the EEA territories, but within the framework of the relevant international law[15]:

'Directive 2000/31, in particular Article 15(1), must be interpreted as meaning that it does not preclude a court of a Member State from:

- *ordering a host provider to remove information which it stores, the content of which is identical to the content of information which was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information;*
- *ordering a host provider to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the*

[9] Azzi, A., 'The challenges faced by the extraterritorial scope of the General Data Protection Regulation', *Journal of Intellectual Property, Information Technology and e-Commerce Law*, Vol. 9, No. 2, 2018, p. 59.
[10] Ibid., p. 60.
[11] Ibid., p. 61.
[12] Ibid., p. 62.
[13] Ibid., p. 63.
[14] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').
[15] CJEU, 3 October 2019, Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18, §53.

injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content, or

- *ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law.'*

Therefore, *mutatis mutandis*, it does not seem impossible to consider that SAs may exercise their investigative (based on the argument *a maiore ad minus*) and corrective powers in a manner that produces effects beyond the EEA territories within the framework of the relevant international law.

However, third countries are bound by neither EU law nor CJEU case-law. It should be reiterated that in the absence of any international convention or treaty or any suitable national legal provision provided in third countries' own legislation, it does not necessarily follow from the interpretation of the CJEU's case-law in the field of eCommerce that:

- third countries will accept SAs exercising investigative and corrective powers in a manner that produces effects on their territories;
- third countries will accept SAs initiating legal actions or proceedings before their courts or tribunals;
- third countries will recognise that SAs are acting in 'civil or commercial matters' or that they are exercising 'public powers';
- the rules applied by SAs when exercising their investigative and corrective powers are 'acceptable' in the third countries' courts or tribunals[16];
- SAs are allowed to send agents abroad to third countries, even with the consent of the controllers/processors established in those countries.

It results from these two preliminary remarks that SAs do not qualify as 'courts or tribunals' in the meaning of Article 267 of the TFEU while exercising their investigative and corrective powers, and they should be considered to exercise 'public powers' under European law only when making use of special powers that go beyond those arising from the ordinary legal rules applicable to relationships between private individuals. It also results from these two preliminary remarks that, in theory, SAs may exercise their investigative and corrective powers in a manner that produces effects beyond the EEA territories, albeit within the framework of the relevant international law.

2.2.3 The enforcement of SAs' investigative and corrective powers in California

It is assumed that European SAs are entitled - or have the power - to engage legal actions outside the EEA, in particular in the US (California), either on the basis of Article 58(5) of the GDPR or their national legislation. Notwithstanding, this subsection considers possible different legal instruments to support enforcement of SAs' investigative and corrective powers.

2.2.3.1 General findings on recognition and enforcement of foreign judgments and administrative acts in the US

(a) <u>The lack of international conventions or treaties on the recognition and enforcement of foreign judgments</u>

[16] See e.g. *mutatis mutandis*: United States Court of Appeals, Yahoo! Inc. v. *La Ligue contre le racisme et l'antisémitisme et l'Union des étudiants juifs de France*, 433 F.3d 1199, 1202 (9th Cir. 2006) (en banc)); M. Chivvis, 'Reexamining the Yahoo! litigations: toward an effects test for determining international cyberspace jurisdiction', *University of San Francisco Law Review*, Vol. 41, 2007, p. 699.

No international convention or treaty facilitates the recognition and enforcement of foreign judgments between the US and any other country[17].

(b) The lack of a federal legislation on the recognition and enforcement of foreign judgments

The US *Congress has passed no law generally regulating the recognition and enforcement of foreign judgments'*[18]. In addition, '*Foreign judgments are not constitutionally entitled to full faith and credit*'[19].

However, no rule prohibits the enforcement of foreign judgments. On the contrary, it seems to be considered that '*the Supreme Court in Hilton v. Guyot suggested long ago that considerations of international comity (recognition and deferral to foreign legislative, executive and judicial acts) may provide a basis for US foreign judgment enforcement'*[20].

(c) Recognition and enforcement of foreign judgments is a matter for State law

Recognition and enforcement of foreign judgments are generally viewed as a matter for State law[21] and are, in principle, ruled by State rather than federal law.

(d) Reciprocity requirement in the matter of recognition and enforcement of foreign judgments

Reciprocity no longer seems to be pivotal element in the recognition and enforcement of foreign judgments[22].

(e) Uncertainty about the court or tribunal in which to bring suits for recognition and enforcement of foreign judgments

It is not always clear whether the suit should be brought before a federal court or a State court. However, even in a federal court, recognition and enforcement remain State law[23].

(f) Some general procedural requirements

The US court, State court or tribunal must have 'subject matter jurisdiction over a case', the case must be 'justiciable' and the US or State court or tribunal must have 'personal jurisdiction' over the defendant[24]. The latter calls for the following observations:

> '*Personal jurisdiction refers to a court's power over the parties in a proceeding. Personal jurisdiction means that a given court has power over a particular defendant. Traditionally, courts based jurisdiction upon territoriality or physical presence in the forum*. (…)'[25].
>
> Personal jurisdiction covers two notions: general jurisdiction and specific jurisdiction: '*General*

[17] Folsom, R., *Principles of International Litigation and Arbitration*, 2d ed., West Academic, Concise Hornbook, 2019, pp. 447-490; Spillenger, Cl., *Principles of Conflict of Laws*, 3d ed., West Academic, Hornbook Series, 2020, pp. 453-454.
[18] Ibid., pp. 453-454.
[19] Ibid., p. 451.
[20] Folsom, R., *Principles of International Litigation and Arbitration*, 2d ed., West Academic, Concise Hornbook, 2019, pp. 447-490.
[21] Ibid., pp. 447-490; Spillenger, Cl., *Principles of Conflict of Laws*, 3d ed., West Academic, Hornbook Series, 2020, p. 453; Bradley, C.A., *International Law in the U.S. Legal System*, 3d ed., Oxford University Press, 2021, pp. 10-11.
[22] Spillenger, Cl., *Principles of Conflict of Laws*, 3d ed., West Academic, Hornbook Series, 2020, pp. 452-453, p 454; Bradley, C.A., *International Law in the U.S. Legal System*, 3d ed., Oxford University Press, 2021, pp. 10-11.
[23] Folsom, R., *Principles of International Litigation and Arbitration*, 2d ed., West Academic, Concise Hornbook, 2019, pp. 447-490.
[24] Bradley, C.A., *International Law in the U.S. Legal System*, 3d ed., Oxford University Press, 2021, pp. 2-8.
[25] Rustad, M., *Global Internet Law*, 3d ed., West Academic, Hornbook Series, 2020, pp. 182-183.

jurisdiction may be used to maintain a suit against a defendant even when it does not arise out of the defendant's activities in the forum state. In contrast, specific jurisdiction allows for a suit to be maintained only when the defendants' contacts with the forum are also the basis for the suit. (…)'[26].

'*General jurisdiction refers to the authority of a court to hear any cause of action involving a defendant, even those unrelated to the defendant's contacts with the forum State. For the court to have general jurisdiction over a corporation, there must be continuous and systematic contacts such as that a corporation is "essentially at home" in the forum state*'[27].

(g) Recognition and enforcement of foreign-country money judgments

When considering the enforcement of SAs' investigative and corrective powers (especially when they impose an administrative fine), consideration must be given to the implementation of the revised version of the 1962 Uniform Foreign-Country Money Judgments Recognition Act[28] (see below, on its implementation in California).

(h) Uncertainties about the scope of the recognition and enforcement of foreign judgments

US courts may recognise a foreign judgment or it may additionally enforce it (wholly or in part)[29], depending on the circumstances of each case.

(i) The law applicable to the suit for the recognition and enforcement of foreign judgments

In any case, there are no clear or settled rules regarding the question of the applicable law. However, it seems that *United States courts will not, however, apply the penal, revenue, or other public laws of foreign nations'* [30].

(j) Recognition and enforcement of administrative acts from foreign nations

The status and regime of administrative acts from foreign nations is unclear:

'*Administrative acts from foreign nations have generally not been treated as judgments except when their review, and the local forum's freedom to alter their result was precluded by supervening executive action or such notions as the "act of state" doctrine. The earlier proposal for a US-UK Recognition-of-Judgments Convention would have expressly limited its application to "judgments" of "courts". On the one hand, the Brussels-I (Recast) Regulation provides that it applies to "civil and commercial matters whatever the nature or tribunal," thereby including administrative tribunals of a judicial nature. Thus, while the recognition provisions (Art. 36 et seq.) only refer to "judgments," it may be true that "the distinction between judgments and administrative acts is generally losing ground together with its obsolescent rationale, and some cases bear this out*'[31].

There is a possibility here for a US or State court or tribunal to recognise that an administrative act from a foreign nation could fall under the notion of 'civil or commercial matters' and be treated as a foreign judgment. To date, however, there is no other indication of the validity of this analysis in either the US

[26] Ibid., pp. 184-185.
[27] Rustad, M., *Global Internet Law*, 3d ed., West Academic, Hornbook Series, 2020, p. 187.
[28] Folsom, R., *Principles of International Litigation and Arbitration*, 2d ed., West Academic, Concise Hornbook, 2019, pp. 447-490.
[29] Ibid., pp. 447-490.
[30] Bradley, C.A., *International Law in the U.S. Legal System*, 3d ed., Oxford University Press, 2021, p. 14.
[31] Hay, P., Borchers, P.J., Symeonides, S.C and Whytock, Chr. A., *Conflict of Laws*, 6th ed., West Academic, Hornbook Series, 2018, p. 1450.

legal doctrine or case-law.

(k) Impact of the 'Act of State Doctrine'

The 'Act of State Doctrine' seems to allow for the recognition of the validity of foreign government acts[32]. Although not relevant for the Study, it is mentioned for the sake of completeness.

2.2.3.2 The 2003 Agreement on mutual legal assistance between the European Union and the United States of America

In 2001, the US and the Republic of Ireland concluded an Agreement relating to mutual legal assistance in criminal matters (Mutual Legal Assistance Treaty or MLAT). Two years later, in 2003, the US and the EU also concluded an Agreement relating to mutual legal assistance in **criminal matters** (the 2003 MLAT).

Article 5 of the 2003 MLAT allows for the constitution and operation of **joint investigative teams** '*for the purpose of facilitating criminal investigations or prosecutions involving one or more Member States and the United States of America where deemed appropriate by the Member State concerned and the United States of America*'[33].

The 2003 MLAT allows for the use of '***video conferencing*** *between each Member State and the United States of America for taking testimony in a proceeding for which mutual legal assistance is available of a witness or expert located in a requested State, to the extent such assistance is not currently available*'[34].

It also provides for mutual legal **assistance** '***to a national administrative authority****, investigating conduct with a view to a criminal prosecution of the conduct, or referral of the conduct to criminal investigation or prosecution authorities, pursuant to its specific administrative or regulatory authority to undertake such investigation. Mutual legal assistance may also be afforded to other administrative authorities under such circumstances. Assistance shall not be available for matters in which the administrative authority anticipates that no prosecution or referral, as applicable, will take place*'[35].

While an EEA SA could try and use 2003 MLAT in cases where violation of a national data protection provision would result in a criminal penalty, it is clear that the 2003 MLAT is not designed to apply to all kinds of cases and its application is not unconditional. In fact, the US authorities do not seem to support the use of MLAT for minor criminal cases.

2.2.3.3 The "Undertaking Spam, Spyware, and Fraud Enforcement With Enforcers beyond Borders Act of 2006' (the 'US Safe Web Act of 2006')

Among other things, the US Safe Web Act of 2006 gives the US Federal Trade Commission (FTC) the authority to provide evidence to foreign law enforcement agencies to support appropriate foreign investigations or enforcement actions.

'*A key requirement is that such proceedings address conduct substantially similar to something that would violate a law the FTC enforces*'[36].

The Act defines foreign law enforcement agencies as:

[32] Bradley, C.A., *International Law in the U.S. Legal System*, 3d ed., Oxford University Press, 2021, pp. 11-14.
[33] Article 5(1) of the 2003 MLAT; Article 5(2 and (4) of the 2003 MLAT for the procedures under which the team is to operate.
[34] Article 6 of the 2003 MLAT.
[35] Article 8(1) of the 2003 MLAT. See Article 8(2) for the transmission of requests.
[36] FTC, Office of International Affairs, US Safe Web Act Information Sheet.

- any agency or judicial authority of a foreign government, including a foreign state, a political subdivision of a foreign state, or a multinational organisation constituted by and comprised of foreign states, that is vested with law enforcement or investigative authority in civil, criminal, or administrative matters;
- any multinational organisation, to the extent that it is acting on behalf of an entity as mentioned above.

On receiving a written request from a foreign law enforcement agency to provide assistance in accordance with this subsection, if the requesting agency states that it is investigating, or engaging in enforcement proceedings against possible violations of laws prohibiting fraudulent or deceptive commercial practices, or other practices substantially similar to practices prohibited by any provision of the laws administered by the Commission, other than Federal antitrust laws, the FTC will provide assistance without requiring that the conduct identified in the request constitute a violation of the laws of the US.

The FTC assistance can consist of:

> *'(A) conduct such investigation as the Commission deems necessary to collect information and evidence pertinent to the request for assistance, using all investigative powers authorised by this Act; and*
> *(B) when the request is from an agency acting to investigate or pursue the enforcement of civil laws, or when the Attorney General refers a request to the Commission from an agency acting to investigate or pursue the enforcement of criminal laws, seek and accept appointment by a United States district court of Commission attorneys to provide assistance to foreign and international tribunals and to litigants before such tribunals on behalf of a foreign law enforcement agency pursuant to section 1782 of title 28, United States Code.'*

In deciding whether to provide such assistance, the FTC must consider all relevant factors, including:

> *'(A) whether the requesting agency has agreed to provide or will provide reciprocal assistance to the Commission;*
> *(B) whether compliance with the request would prejudice the public interest of the United States; and*
> *(C) whether the requesting agency's investigation or enforcement proceeding concerns acts or practices that cause or are likely to cause injury to a significant number of persons.'*

The US Safe Web Act of 2006 provides that '*If a foreign law enforcement agency has set forth a legal basis for requiring execution of an international agreement as a condition for reciprocal assistance, or as a condition for provision of materials or information to the Commission, the Commission, with prior approval and ongoing oversight of the Secretary of State, and with final approval of the agreement by the Secretary of State, may negotiate and conclude an international agreement, in the name of either the United States or the Commission, for the purpose of obtaining such assistance, materials, or information. The Commission may undertake in such an international agreement to*:

(A) provide assistance using the powers set forth in this subsection;
(B) disclose materials and information in accordance with subsection (f) and section 21(b); and
(C) engage in further cooperation, and protect materials and information received from disclosure, as authorized by this Act'[37].

Application of the US Safe Web Act of 2006 has been extended until 30 September 2027.

[37] Section 6 of the US Safe Web Act of 2006, on the sharing of information with foreign law enforcement agencies.

Again, it is quite clear that the US Safe Web Act of 2006 is not designed to tackle all kind of situations and its application is not unconditional. Rather, it was designed for important criminal cases and not for what could be perceived by the US as minor criminal cases.

The Data Protection Commissioner of Ireland and the Dutch Data Protection Authority have concluded MoUs with the FTC in the matter of the enforcement of laws protecting personal information in the private sector[38], referring e.g. to the US Safe Web Act of 2006.

2.2.3.4 The 2018 Clarifying Lawful Overseas Use of Data Act (the Cloud Act)

After several cases and legal disputes involving warrants to search data stored outside the US - notably in the EU[39] - the US adopted the 2018 Cloud Act.

In application of the 2018 Cloud Act, foreign governments may ask for the communication of data stored in the US when complying with several conditions, including the conclusion of an Executive Agreement with the US:

> '*It shall not be unlawful under this chapter for a provider of electronic communication service to the public or remote computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523'*[40].

With respect to this, the US Department of State explains e.g. that:

- The Cloud Act aims to speed up access to electronic information held by US-based global providers that is critical to US foreign partners' investigations of serious crime, ranging from terrorism and violent crime to sexual exploitation of children and cybercrime;
- The Cloud Act is designed to permit US foreign partners that have robust protections for privacy and civil liberties to enter into bilateral agreements with the US to obtain direct access to this electronic evidence, wherever it happens to be located, in order to fight serious crime and terrorism;
- The Cloud Act authorises bilateral agreements between the US and trusted foreign partners that will make both nations' citizens safer, while at the same time ensuring a high level of protection of those citizens' rights.

To date, no executive agreement relating to the Cloud Act has been concluded between the US and the EU. It is not clear whether the EU is precluded from concluding this kind of executive agreement and if, in fact, such an agreement might only be possible between the US Government and each Member State acting separately[41]. In any case, the EU Commission has entered into negotiations for the conclusion of an EU-US agreement to facilitate access to electronic evidence in criminal investigations.[42]

---

[38] Cf. https://www.ftc.gov/system/files/documents/cooperation_agreements/150309ftcdutchcb-1_0.pdf ; https://www.ftc.gov/system/files/documents/cooperation_agreements/130627usirelandmouprivacyprotection.pdf

[39] For example, the brief of the European Commission on behalf of the European Union as *Amicus Curiae* in support of neither party – United States of America v. Microsoft Corporation (US Court of Appeals, 2e Circuit), n° 17-2.

[40] US Code, Title 18, Chapter 119, Section 2511(2)(j).

[41] On this point cf. e.g.Cassart, A., 'Premières réflexions sur le Cloud act: contexte, mécanismes et articulations avec le RGPD', Bruxelles, Larcier, *Revue du droit des technologies de l'information*, No. 73, 2018, p. 49.

[42] Cf. https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/ and https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

2.2.3.5 The Californian Uniform Foreign-Country Money Judgments Recognition Act

The Californian Uniform Foreign-Country Money Judgments Recognition Act only applies to foreign judgments that grant or deny recovery of a sum of money. However, it does not apply to a foreign-country judgment, even if the latter grants or denies recovery of a sum of money, to the extent that the judgment is a fine or any other penalty[43]. Provision 1723 of the California Code of civil Procedure (CCP) specifies that Chapter 2 does not prevent the recognition under principles of comity or otherwise of a foreign-country judgment not within its scope.

2.2.3.6 The California Consumer Privacy Act of 2018

In 2018, the State of California adopted the California Consumer Privacy Act[44]. According to this act, the California Privacy Protection Agency is invested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018.

Among other things, the California Privacy Protection Agency shall '*Cooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in other states, territories, and countries to ensure consistent application of privacy protections*'[45].

The California Privacy Protection Agency thus seems to be a natural correspondent for the EU SAs in the enforcement of their investigative and corrective powers.

2.2.3.7 Key findings

The enforcement of EU SAs' decisions in California courts may prove difficult if not impossible in a reasonable timeframe and without prejudice to its financial cost. However, the adoption of the California Consumer Privacy Act of 2018 may open the door to an active cooperation with the California Privacy Protection Agency.

2.2.4 The enforcement of SAs' investigative and corrective powers in the UK

This subsection presents a short introduction to the UK data protection legal framework and then considers different legal instruments that could support the enforcement of SAs' investigative and corrective powers.

2.2.4.1 UK Data Protection Legal Framework: DPA 2018 and the UK GDPR

The EU GDPR no longer applies to the UK. The UK Data Protection Act 2018 (DPA 2018) sets out the framework for the protection of personal data in the UK. It came into effect on 25 May 2018, and was amended on 1 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

The provisions of the EU GDPR have been incorporated into UK law as the UK GDPR. The DPA 2018 sits alongside and supplements the UK GDPR. The UK GDPR is a UK law which came into effect on 1 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for processing by law enforcement and intelligence agencies.

The EU GDPR still applies to UK controllers/processors operating in the EEA, offering goods or

[43] California Code of Civil Procedure – CCP, Part 3. Of Special Proceedings of a Civil Nature, Title 11. Money Judgments of other jurisdictions, Chapter 2. Foreign-Country Money Judgments, §§1713-1725.
[44] State of California, Civil Code, Division 3. Obligations. Part 4. Obligations arising from particular transactions. Title 1.81.5. California Consumer Privacy Act of 2018, § 1789.199.10.
[45] Id., §1789.199.40(i).

services to individuals in the EEA, or monitoring the behaviour of individuals in the EEA. UK controllers/processors thus may need to comply with both the UK GDPR and the EU GDPR.

On 28 June 2021, the EU approved adequacy decisions for the EU GDPR and the Law Enforcement Directive (LED)[46]. Both decisions are expected to remain in force until 27 June 2025.

The Information Commissioner's Office (ICO) (the UK Data Protection Supervisory Authority) states that it is not the regulator for any European-specific activities captured by the EU GDPR[47].

2.2.4.2 Selected ICO Commissioner functions and missions that could be of interest in the enforcement of EU SAs' investigative and corrective powers in the UK

(a) Investigation on the basis of information received from a foreign authority

According to Article 57(1)(h) of the UK GDPR, the Commissioner must '*conduct investigations on the application of this Regulation, including on the basis of information received from a foreign designated authority or other public authority'*.

(b) Inspection on the basis of an international obligation of the UK

According to Article 119(1) of the DPA 2018, '*The Commissioner may inspect personal data where the inspection is necessary in order to discharge an international obligation of the United Kingdom, subject to the restriction in subsection (2)*.'

'*The power under subsection (1) includes power to inspect, operate and test equipment which is used for the processing of personal data*'[48].

Excepted for urgent cases, '*the Commissioner must by written notice inform the controller and any processor that it intends to exercise power under subsection* (1)'[49].

(c) International cooperation

Article 120 of the DPA 2018 confers on the Commissioner a further international role in connection with the processing of personal data to which the UK GDPR does not apply.

For the processing of personal data to which the UK GDPR does apply, the DPA 2018 refers to Article 50 of the UK GDPR:

> *'In relation to third countries and international organisations, the Commissioner shall take appropriate steps to:*
>
> *(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;*
> *(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;*
> *(c) engage relevant stakeholders in discussion and activities aimed at furthering*

[46] EU 28 June 2021 Decision on the adequate protection of personal data by the United Kingdom - General Data Protection Regulation; EU 28 June 2021 Decision on the adequate protection of personal data by the United Kingdom: Law Enforcement Directive.
[47] source: the ICO website.
[48] Article 119(3) of the DPA 2018.
[49] Article 119(4) and (5) of the DPA 2018.

international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.'

2.2.4.3 UK MoUs in the field of data protection

The UK ICO has concluded several MoUs in the field of data protection[50]:

- 2019 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and Canadian Radio-television and Telecommunications Commission for cooperation in the enforcement of laws protecting personal data;
- 2019 MoU between the Personal Data Protection Commission of the Republic of Singapore and the Information Commissioner for the United Kingdom for cooperation in the enforcement of laws protection personal data;
- 2020 US FTC and UK ICO MoU on mutual assistance in the enforcement of laws protection personal information in the private sector;
- 2020 MoU between the Privacy Commissioner of Canada and the Information Commissioner of the United Kingdom on mutual assistance in the enforcement of laws protecting personal information in the private sector;
- 2020 MoU between the Privacy Commissioner for Personal Data of Hong Kong, China and the Information Commissioner for the United Kingdom for cooperation in protection personal data;
- 2020 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and the New Zealand Department of Internal Affairs for cooperation in the regulation of unsolicited electronic messages;
- 2020 MoU between the Information Commissioner and the Global Cyber Alliance;
- 2021 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and the Office of the Privacy Commissioner for New Zealand for cooperation in the enforcement of laws protecting personal data;
- 2021 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and the National Privacy Commission of the Philippines for cooperation in the regulation of laws protecting personal data.

The content of these MoUs is not always strictly the same but some patterns are evident, such as sharing experience, investigative and enforcement assistance, and joint investigations. For instance, the MoU with the Canadian Radio-television and Telecommunications Commission covers sharing experience, exchanging information and joint investigations (excluding sharing personal data) but does not seem to be legally binding. The MoU with the US FTC covers the provision of investigative assistance in appropriate cases, sharing information, coordinating enforcement against certain cross-border privacy violations, etc. However, the assistance is not limitless, absolute or unconditional.

2.2.4.4 Enforcement of SAs' investigative and corrective powers falling within the scope of 'civil and commercial matters'

There is no indication from the answers received from the SAs to the questionnaire nor from the desk research whether SAs do or do not have the power to engage legal actions abroad either on the basis of Article 58(5) of the GDPR or under their national legislation. The answer to this question should be investigated under the rules governing the actions of the SAs including the possibility under the UK law for a foreign 'administrative' body to initiate legal actions in the UK.

[50] These MoUs can be found on the ICO website: https://ico.org.uk/about-the-ico/our-information/working-with-other-bodies/

In any case, if the enforcement of SAs' investigative and corrective powers is considered to fall within the scope of the notion of 'civil and commercial matters' (see section 2.2.1.2) (from a EU perspective) and accepted as such under UK law, EU SAs could consider the UK legal regime on recognition and enforcement of foreign judgments[51] (see section 2.5.7 and section 2.2.1.2 for a discussion of whether SAs could be considered to act as private persons when they are not exercising 'public powers' under the accepted meaning in EU law, especially CJEU case-law analysis).

(a) International conventions or treaties in the matter of the recognition and enforcement of foreign judgments in the UK

The UK is a party to the Hague Convention on Choice of Court Agreements 2005 since 28 September 2020. As of the end of the Brexit transition period on 31 December 2020, however, it is no longer a party to the Lugano Convention 2007.

The UK is not a signatory to the Hague Convention on the recognition and enforcement of foreign judgments in civil and commercial matters 1971, nor to the Hague Convention on the recognition and enforcement of foreign judgments in civil or commercial matters 2019[52].

The Hague Convention on Choice of Court Agreements 2005 does not seem an easy avenue to base a choice of jurisdiction between SAs and third-country controllers or processors.

(b) UK law on recognition and enforcement of foreign judgments

The Foreign Judgments (Reciprocal Enforcement) Act 1933 applies to judgments from courts in Australia, Canada (except Quebec and Nunavut), India, Israel, Pakistan, Guernsey, Jersey and the Isle of Man, and to judgments from some European countries (Austria, Belgium, France, Germany, Italy, the Netherlands, Norway).

Common law relating to the recognition and enforcement of foreign judgments applies where the jurisdiction from which the judgment relates does not have an applicable treaty in place with the UK or in the absence of any applicable UK statute. This typically refers to the US, China, Russia and Brazil. The addition of the EU to this list could be considered.

However, it is not clear whether any of these could support the enforcement of SAs' investigative and corrective powers in the UK.

2.2.4.5 Key findings

The enforcement of EU SAs' decisions in the UK courts may prove difficult - if not impossible - in a reasonable timeframe and without prejudice to financial cost. However, cooperation with the UK Data Protection Commissioner seems possible through the prism of Treaty 108+ (Articles 16 and 17), combined with the functions and missions vested in the UK Commissioner by the UK GDPR and DPA 2018. It is worth noting that the UK Commissioner has concluded a relatively high number of MoUs with foreign data protection authorities.

2.2.5 The enforcement of SAs' investigative and corrective powers in China

2.2.5.1 The Chinese legal framework in the matter of data protection

The Personal Information Protection Law (PIPL) was adopted on 20 August 2021 and will come into

[51] On this topic, please cf. e.g. Cheshire, North & Fawcett, *Private International Law*, 15th ed., Oxford University Press, 2017; Browne, O. and Watret, T., *Enforcement of foreign judgments*, 10th ed., London, Law Business Research, Lexology, 2020.

[52]

force on 1 November 2021. The PIPL should not be read in isolation but in combination with other Chinese laws that together comprise the Chinese data protection legal framework. Particular attention should be paid to the Data Security Law passed on 10 June 2021, which will come into force on 1 September 2021.

The scope for international assistance in the PIPL is not clear:

> '*If it is necessary to transfer personal information outside of China for international judicial assistance or administrative law enforcement, information handlers must file an application with the relevant competent authority for approval (Art. 41). The law stipulates that international treaties or agreements that China has become party to may govern cross-borders transfers and supersede the provisions of the law. It is not clear if this provision only concerns international judicial assistance, or also includes general cross-borders data transfers*.'

The PIPL does not create an independent authority dedicated to its enforcement. Rather, the primary agency for data protection appears to be the Cyberspace Administration of China (CAC), but there are other regulators.

Of note is that in the event of a violation of the PIPL, the People's Procuratorates[53], and other relevant enforcing authorities may file a suit with a People's Court. However, at this stage, we have no information as to whether foreign authorities might ask for their cooperation or file a suit with a People's Court[54].

2.2.5.2 The recognition and enforcement of foreign judgments in China

The recognition and enforcement of foreign judgments in China might prove difficult:

> '*In China, in theory, recognition and enforcement of foreign judgment ("REJ") are possible if there is, among other conditions, a treaty of mutual judicial assistance or reciprocity. Until recently, it was almost impossible to obtain REJ absent a treaty of mutual judicial assistance, which is rare and usually focused on criminal cases. However, lately, Chinese courts have shown more willingness to enforce foreign judgment on the basis of reciprocity and have adopted a pro-active attitude in triggering the reciprocity cycle*'[55].

There might be a need to establish some common grounds with Chinese values:

> '*Beyond comity and reciprocity, the existence of shared values of privacy protection with the foreign jurisdiction and the legitimacy of the extraterritorial claim will significantly impact the likelihood of foreign enforcement. The more limited the nexus for jurisdiction is, the more likely it is that the foreign jurisdiction will not enforce the decision'*[56].

There might be unexpected consequences to the denial of recognising and enforcing foreign judgments:

> '*Jurisdictional claims regarded as illegitimate (…) may even lead to the adoption of a "blocking statute". Such legislation may forbid the production of evidence or any documents in foreign proceedings, prohibit compliance with orders of foreign authorities, etc.* (…)'[57].

[53] The People's Procuratorates of the People's Republic of China are state organs for legal supervision.
[54] Dorwart, H., Zanfir-Fortuna, G. and Girot, C., 'China's new comprehensive data protection law: context, stated objectives, key provisions', *Future of Privacy Forum*, 20 August 2021; Greenleaf, G., *Asian Data Privacy Laws. Trade and Human Rights Perspectives*, Oxford University Press, 2017, pp. 218-219.
[55] Azzi, A., 'The challenges faced by the extraterritorial scope of the General Data Protection Regulation', *Journal of Intellectual Property, Information Technology and e-Commerce Law*, Vol. 9, No. 2, 2018, p. 66.
[56] Ibid., p. 67.
[57] Ibid., p. 68.

However, it seems that there could be some possibilities to enforce SAs' investigative and corrective powers to some extent:

> '*In conclusion, cooperation with foreign jurisdiction may be relied on for the enforcement of the GDPR outside Europe to the extent that the jurisdictional claim is reasonable and legitimate (and with the consent of the State for investigation measures). It follows that it would probably require more than the mere utilisation of cookies to enforce a judgment abroad through the sole means of international cooperation*'[58].

2.2.5.3 Key findings

Cooperation with China seems possible in theory but would require a comprehensive approach, including close cooperation with EU and Member State public authorities responsible for the relationship with China.

2.3 IDENTIFICATION OF LEGAL INSTRUMENTS THAT COULD SUPPORT ENFORCEMENT OF THE GDPR

Section 2.3.1 presents the legal instruments that could support enforcement of the GDPR against a controller/processor, based on SAs' questionnaire responses. These legal instruments could be relied on when enforcing the GDPR against a controller/processor established in the US, UK or China that falls under Article 3(2), and in the recognition and enforcement of SAs' investigative and corrective powers.

Section 2.3.2 refers to other legal instruments, which, while not quoted by the SAs, could support enforcement of the GDPR against a controller/processor that falls under the scope of Article 3(2) GDPR but is not willing to cooperate with SAs and did not designate an EEA representative.

2.3.1 Legal instruments identified by SAs

2.3.1.1 Bulgarian SA

- 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);
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications);
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) (for cooperation, assistance, decision notification);
- Personal Data Protection Act;
- European Convention on Human Rights (ECHR) (cooperation);
- Universal Declaration of Human Rights;
- Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime;
- Regulation 2019/788 (cooperation);
- Regulation 611/2016 (cooperation);
- Charter of Fundamental Rights (cooperation);
- Rules on the activity of the Commission for Personal Data Protection and its administration.

[58] Ibid., p. 69.

2.3.1.2 Finnish SA

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) (for cooperation);
- Data Protection Act (1050/2018) (18a§) (cooperation in the framework of T108);
- Organisation for Economic Co-operation and Development (OECD) Guidelines (cooperation and mutual assistance).

2.3.1.3 French SA

The legal instruments that could be used with third countries to enforce the GDPR are either a legally binding agreement or a non-binding administrative arrangement (bilateral or multilateral) (Articles 46(3)(a) and 46(3)(b) of the GDPR).

However, under the French legal order, the French SA would not be able to use instruments labelled MoU, but could only conclude administrative arrangements (deriving from public international law and principles).

2.3.1.4 Italian SA

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) (only for the UK).

2.3.1.5 Luxemburg SA

There is no specific legal instrument on which the Luxembourgish SA might rely. The national SA specified that international cooperation mechanisms with the US or other third-country officials under Article 50 GDPR are not yet concrete, either at EU or national level.

The national SA (CNPD) has no legal power under national law to initiate the drafting of a legally binding and enforceable instrument between public authorities or bodies with the objective of establishing an effective international cooperation channel[59] with guarantees for the transfer of personal data of the complainant to third countries[60].

The CNPD is limited by legal professional secrecy, as it cannot share information with other public entities unless those entities have similar professional secrecy obligations[61].

At national level, only the government or parliament has the legal power to adopt legally binding and enforceable international instruments.

2.3.1.6 Polish SA

- Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community.

2.3.2 Other instruments to consider

Other instruments should also be considered as potentially supporting the enforcement of SA investigative and corrective powers abroad:

- Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018

[59] Article 50 GDPR.
[60] Article 46(2) of the GDPR.
[61] Articles 42-44 of the Luxembourg Act of 1 August 2018.

on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC;

- Articles 16 and 17 of the Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Treaty 108+), on Cooperation and Mutual Assistance: sharing of information, joint actions or investigations (compare with the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (8 November 2001, ETS n° 181) (the UK has signed but not yet ratified Treaty 108+) (the US and China are not party to Treaty 108+);
- OECD 2007 Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy;
- OECD 2020 Summary of Discussion, 'Roundtable on Legislative Initiatives to Improve Cross-border Enforcement Cooperation' (DSTI/CP(2019)21/FINAL);
- OECD 2012 Background Note on Improving International Co-operation in Cartel Investigation (DAF/COMP/GF(2012)6));
- International Conference of Data Protection and Privacy Commissioners (ICDPPC), 2017 Global Cross-border Enforcement Cooperation Agreement, version 17);
- Global Privacy Enforcement Network 2013, Action Plan for the Global Privacy Enforcement Network (GPEN);
- Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Enforcement Arrangement (CPEA)

2.3.3 Key findings

There is not a clear view from the SAs' perspective on the legal instruments that could support the enforcement of the GDPR against third-country controllers and processors. However, it could be interesting to investigate further the effectiveness and efficiency of the GPEN while considering the experiences from the ICDPPC Enforcement Cooperation Agreement and the APEC Enforcement Arrangement. It is worth noting, for example, that the Office of the Australian Information Commissioner, the Office of the Victorian Information Commissioner, the New Zealand Office of the Privacy Commissioner, the US FTC, the Office of the Privacy Commissioner for Personal Data, Hong Kong, China, the Office of the Privacy Commissioner of Canada, are all CPEA participants.

2.4 SHARING SAS' EXPERIENCES AND IDENTIFICATION OF OTHER TYPES OF ACTIONS

Section 2.4.1 details the experiences reported by SAs in their answers to the questionnaire.

Section 2.4.2 describes other types of actions suggested by the SAs responding to the questionnaire, as well as other types of actions discussed in the legal literature.

2.4.1 Sharing SAs' experiences

2.4.1.1 Czech SA

In its previous investigations, controller/processor established in a country beyond the EEA zone always had a representative, in accordance with Article 27 of the GDPR. The Czech SA has yet to deal with a situation where it would be necessary to work directly with a controller/processor to enforce the GDPR.

2.4.1.2 Estonian SA

The Estonian SA received a request for assistance from a foreign data protection authority, asking it to provide investigation files of a case already decided by the Estonian courts. The request was deemed to be driven by political interests and the Estonian SA denied the request on the basis that there was no

legal ground for the demand.

2.4.1.3 Finnish SA

The Finnish SA's experience regarding entities outside the EEA that fall under Article 3(2) GDPR is limited to erasure requests from Google, for example, which did not require measures directly on the territory of a third country.

2.4.1.4 French SA (CNIL)

Two years ago, the CNIL was warned about the potential illegal collection of data on several websites and apps. It conducted online investigations and notified the data controller, which was established in the US. The CNIL then summoned the data controller to a hearing before its own department of investigation. The data controller attended the hearing and the proceeding is ongoing.

In a specific case where the CNIL could not clearly identify the data controller of a website but the data processor was identified as a Moroccan company, the CNIL asked its colleagues in the Moroccan data protection authority to perform an on-site investigation at the data processor's facility and inform the CNIL of its findings. The data controller was a company in Brazil and the CNIL chose not to continue the investigation as it would not have been able to enforce corrective powers on a Brazilian company.

In a third case, the CNIL received complaints about a major data breach concerning French data subjects (among others). It undertook an online investigation to confirm the data breach and lack of security. It then notified the data controller and asked several questions about the data breach. When the data controller failed to reply, the CNIL sent a letter to remind it of its legal obligations. The CNIL was not able to enforce its corrective powers.

In three separate cases, requests from non-European data protection authorities were handled informally via phone call or email exchanges. No information was disclosed, but the CNIL could advise the other authorities of the investigation and the stakes of the procedure in order to help them with their own investigations. The CNIL also discussed its method of investigation (e.g. how it conducts online investigations) and the tools used.

2.4.1.5 Croatian SA

The Croatian SA has only received inquiries from third countries about the interpretation of the provisions of the GDPR.

2.4.1.6 Italian SA

In 2015, in relation to some processing activities carried out by Google Inc. that fell under the scope of application of Article 4 Directive 95/46, the Italian SA sent a small team of IT and legal officers to the company headquarters in the US, on the basis of a verification protocol signed with the company and referenced in a decision adopted by the Garante in July 2014 to verify whether the measures implemented by the US controller were in compliance with Italian law.

The protocol envisaged quarterly updates on progress from the controller and empowered the Italian SA to carry out on-the-spot checks at Google´s US headquarters. All information provided through progress updates or directly by the company during the on-the-spot check of the Garante was used to assess the implementation of the measures adopted by the Garante in its decision of 10 July 2014. The final decision of the Garante of 29 July 2016 is not available in English, however.

2.4.1.7 Lithuanian SA

The Lithuanian SA had no cases relating to a controller/processor established in the US, UK or China. It did, however, have a case regarding a controller established in Seychelles. The Lithuanian SA sent questions to a controller but no answers were provided and the case was dismissed. Although the GDPR application might be extraterritorial, the exercise of investigating powers against a controller/processor established outside the EU depends on the willingness of a controller/processor to provide answers.

2.4.1.8 Luxemburg SA

To date, the Luxembourg SA has only had experiences with entities established in the US. Considering its lack of effective enforcement powers on the US territory in practice, the SA usually makes informal contact with the controller/processor by post and email in order to try to reach a solution based on cooperation. Prior to that contact, it usually assesses whether it is possible to address the data protection issue with the controller/processor without disclosing any personal data. Where that is not possible (usually in the context of a complaint), the SA requests data subjects' consent under Article 49(a) GDPR to allow the transfer of their personal data in the US, in the absence of an adequacy decision pursuant to Article 45(3) GDPR or appropriate safeguards pursuant to Article 46 GDPR in national and EU law. Should the data subject refuse to consent, the SA is unable to process its complaint further. In some cases, the lack of effective enforcement powers of the SA makes it difficult to establish the applicability of Article 3(2) GDPR to the concerned entity, due to lack of available information or the possibility of obtaining that information if the concerned entity refuses to cooperate, in particular where the entity has not appointed a representative under Article 27 GDPR.

2.4.1.9 Polish SA

The Polish SA had some experience in sending requests for information to entities based in the US in the course of proceedings on complaints about violation of the provisions of the GDPR, specifically the transfer of personal data to the US without a legal basis (following the judgment of the CJEU in the Schrems II case).

For example, one of the organisations (private sector) conducted activities focused on European data subjects. This organisation is beyond the EEA. Under Article 58(1a) and (1e) of the GDPR, the Polish SA asked the organisation to answer the following questions: does the company have a representative for the processing of personal data in the EU, and if so, please provide its data? Who is the controller of personal data obtained from a controller's website? Whether the information is publicly available, and if so, please provide a precise indication? Does the company process personal data of citizens or other persons residing in the Republic of Poland? On what legal basis does the company process personal data of the above persons? What supervisory authority is mentioned in the privacy policy posted in the controller's website?

The US-based entity answered the authority's request as required. The entity's letter was drawn up in Polish, as required by Polish national law, and within the prescribed period. The entity appointed a proxy (legal attorney – resident of Poland) to represent the controller before the President of the Personal Data Protection Office.

2.4.1.10 UK ICO

In 2018, the UK ICO served a first enforcement notice to the company AIQ Ltd., which had no physical presence in the EU (known as the Cambridge Analytica scandal). The notice was based on Article 3(2) of the EU GDPR. The notice required AIQ Ltd. to cease processing any personal data of EU citizens obtained from organisations or otherwise, for the purposes of data analytics, political campaigns or any advertising purposes. The scope of the second notice was narrowed to individuals in the UK. AIQ Ltd. was given 30 days to comply before facing a fine of EUR 20 million or 4% of its global turnover,

whichever was the higher.

2.4.2 Identification of other types of action and SAs' observations

2.4.2.1 Other types of action suggested by SAs

(a) Bulgarian SA

The Bulgarian SA stated that the current system of rules and procedures, together with experience and administrative capacity, should create enough safeguards to ensure enforcement of the GDPR provisions.

(b) French SA

An efficient measure would be for SAs to order the internet service providers within their jurisdiction to deny access to a particular domain name (or to redirect connections to a warning page).

(c) Croatian SA

Raising awareness among all controllers, including those from third countries that provide their services to data subjects in the EEA.

(d) Italian SA

The Garante does not have the power to order an internet connectivity service provider to inhibit access from Italy to websites collecting personal data unlawfully (this power was recently conferred on the Italian authority responsible for regulating the Italian financial markets (Consob) in cases where financial services are offered without due authorisation), but this power could perhaps be useful.

An order to stop collecting/processing personal data by means of a website could be adopted by the SA as one of the corrective measures under Article 58(2) of the GDPR. Like the other corrective measures, however, it will be difficult to enforce in respect of an Article 3(2) controller/processor.

(e) Polish SA

Imposition of the restriction of processing of personal data of EU citizens.

(f) Slovakian SA

The Slovakian stated that effective enforcement needs an entity in the EEA against which the SA could exercise the corrective powers in the territory where this entity is established or has a representative.

2.4.2.2 Other types of action suggested in the legal literature

Other types of action are suggested in the legal literature:

- Asset-freezing orders when controllers/processors possess assets in the EU[62];
- 'Market destroying measures' to penalise the operator (prohibiting the party from trading within the jurisdiction or making debts owed to that party unenforceable within the

[62] Azzi, A., 'The challenges faced by the extraterritorial scope of the General Data Protection Regulation', *Journal of Intellectual Property, Information Technology and e-Commerce Law*, Vol. 9, No. 2, 2018, p. 70.

jurisdiction)[63];

- Obtaining a court injunction against the local business partners that are indirectly using the processed personal data[64];
- Obtaining a court injunction blocking the websites of the operator or its partners, or the associated internet connections (via injunctions applied to internet service providers)[65];
- Encouraging codes of conduct[66].

The legal literature reported that the Belgian SA has concluded an agreement with a not-for-profit private association that registers domain names. Under that agreement, the association will enforce the Belgian SA's decision to block internet sites with a (.be) extension.

2.4.3 Key findings

SAs have gained some experience of international cooperation, albeit informally. They identified some avenues to improve international cooperation in data protection. Direct action against the electronic communications infrastructure or the intermediaries located in EEA territories (e.g. order to stop collecting personal data or order to shut down a website) appears to be most effective.

2.5 ANALYSIS OF THE POSSIBILITY TO RELY ON UNILATERAL COMMITMENTS FROM CONTROLLERS/PROCESSORS IN THE MATTERS OF CHOICE OF JURISDICTION AND APPLICABLE LAW

This subsection analyses the possibility to rely on controllers'/processors' commitments in the matters of choice of jurisdiction and applicable law, based on the existence of a mutual agreement, a clause in BCR, or a unilateral commitment from controllers/processors.

The validity of controllers/processors commitments established in California or the UK is analysed through the prism of EU law but not US/California law or UK law. The information for this section is drawn from SAs' responses to the questionnaire.

Sections 2.5.1 – 2.5.3 discuss the choice of jurisdiction in an agreement between a controller/processor from a third country and an EEA SA (Section 2.5.1), in the BCR (Section 2.5.2), and in a unilateral commitment from the controller/processor (Section 2.5.3).

Sections 2.5.4 – 2.5.6 discuss the choice of applicable law in case of an agreement (Section 2.5.4), BCR (Section 2.5.5) or unilateral commitment (Section 2.5.6).

Finally, **Section 2.5.7** describes the impact of the CJEU's interpretation of the notion of 'civil and commercial matters' where that notion could apply to EEA SAs exercising their powers abroad.

2.5.1 Possibility for an agreement between controllers/processors and SAs on choice of jurisdiction

SAs did not recognise the possibility of an agreement with controllers/processors on the choice of jurisdiction.

The French SA observed that '*Since we are in a 3(2) scenario, the European framework does not allow for a choice of jurisdiction as this is covered directly by the GDPR. Therefore, private international law principles cannot apply in this case*.'

[63] Ibid., p. 72.
[64] Ibid., p. 73.
[65] Ibid., p. 73.
[66] Ibid., p. 78 et seq.

The Italian SA considered that '*Article 78.3 GDPR already identifies the relevant jurisdiction for proceedings against an SA and we are not sure the SA may "derogate" from this provision*.'

2.5.2 Possibility to rely on a choice of jurisdiction in BCR

SAs' responses in respect of the possibility to rely on a choice of jurisdiction in BCR were more diverse. It seems possible for the Bulgarian, the Finnish and the Italian SAs (to some extent), but not possible for the Czech and French SAs (the latter for the same reasoning as in Section 2.5.1).

However, the Italian SA specified that, '*According to Article 47.2.e GDPR, an EEA SA will be competent for complaints lodged with it by a data subject for cases where a violation of the BCRs has been carried out by a third country BCR member, i.e. the third country BCR member accepts an EEA SA's and/or court's jurisdiction for such cases. By the same token, for example, they accept to comply with any EEA competent SA's decision or advice relating to compliance with/interpretation of the BCRs. BCRs cannot contain provisions according to which a SA shall accept any other jurisdiction than its own. With regard to the enforcement against an Article 3.2 controller/processor, the jurisdictions referred to in the BCRs could be relevant only for cases where the SA will have to assess compliance with the commitments contained in the BCR for transfers and onward transfers carried out by the same Article 3.2 controller/processor*.'

2.5.3 Possibility to rely on a choice of jurisdiction in a unilateral commitment from controllers/processors

Most of the SAs that responded to the questionnaire did not recognise the possibility of a choice of jurisdiction in a unilateral commitment from controllers/processors (the French SA repeating the same reasoning as in Section 2.5.1).

However, the Italian SA considers that '*BCRs, commitments taken by means of unilateral declarations can be taken into account only under certain conditions specified in the WP 256 and 257 (BCR Referentials). This also applies to the commitment to accept the jurisdiction of the Italian SA and/or an Italian court*.'

2.5.4 Possibility for an agreement between controllers/processors and SAs on choice of the applicable law

Most of the SAs that responded to the questionnaire did not recognise the possibility of an agreement between controllers/processors and SAs on the choice of applicable law (the French SA repeating the same reasoning as in Section 2.5.1).

2.5.5 Possibility to rely on a choice of applicable law in BCR

Most of the SAs that answered the questionnaire did not recognise the possibility to rely on a choice of applicable law in BCR (the French SA repeating the same reasoning as in Section 2.5.1).

However, the Italian SA noted that '*We can rely on the choice made by a third-country BCR member to accept the Italian law as the one applicable to their processing of personal data transferred from the Italian territory under the BCRs*.'

2.5.6 Possibility to rely on choice of applicable law in a unilateral commitment from controllers/processors

With the exception of the Italian SA, most of the SAs that responded to the questionnaire did not recognise the possibility to rely on a choice of applicable law in a unilateral commitment from controllers/processors (the French SA repeating the same reasoning as in Section 2.5.1).

2.5.7 Impact of CJEU interpretation of the notion of 'civil and commercial matters'

Situations where SAs are not exercising public powers when exercising their investigative and corrective powers (see Section 2.2.1.2) could be within the scope of the notion of 'civil and commercial matters'. The application of Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, as well as Regulation (EC) No 593/2008 on the law applicable to contractual obligations (Rome I), could therefore be considered.

If this possibility is confirmed, SAs and controllers/processors could rely on Article 25(1) of the Regulation No 1215/2012 to agree on a choice of jurisdiction, the latter providing that:

> *'If the parties, regardless of their domicile, have agreed that a court or the courts of a Member State are to have jurisdiction to settle any disputes which have arisen or which may arise in connection with a particular legal relationship, that court or those courts shall have jurisdiction, unless the agreement is null and void as to its substantive validity under the law of that Member State. Such jurisdiction shall be exclusive unless the parties have agreed otherwise*. (…)'

Similarly, SAs and controllers/processors could rely on Article 3 Regulation No 593/2008 to agree on the applicable law. This choice is not necessarily limitless or unconditional (please cf. Article 3(3-5)).

2.5.8 Key findings

It appears quite difficult for SAs to rely on unilateral commitments from controllers and processors on the choice of jurisdiction or applicable law. However, if SAs are to be considered as acting in 'civil and commercial matters', there could be some discussion about the possibility for some degree of choice of jurisdiction or applicable law.

2.6 IMPORTANCE OF CONTROLLER/PROCESSOR REPRESENTATIVES

This subsection analyses the added value and limits of controllers/processors' representatives, as perceived by SAs (see **Section 2.6.1** and **Section 2.6.2**, respectively). The analysis is based on SAs' responses to the questionnaire and includes their experiences with EEA representatives (**Section 2.6.3**). **Sections 2.6.4** discusses the scope of representatives' obligations under the GDPR.

2.6.1 Added value of controller/processor representatives in the experience of SAs

The majority of the SAs that responded to the questionnaire underlined the importance of the designation of a representative for controllers/processors that fall under the scope of Article 3(2) GDPR. They stressed that:

- The representative provides a direct link to the controller, acts as a contact point for SAs (e.g. notification of a corrective measure) and data subjects, and facilitates communication (BG, FI, FR, HR, HU, IT, PL);
- The representative may be addressed in addition/instead of the controller/processor by the SA on all issues related to processing, for the purposes of ensuring compliance with the GDPR. The powers of the SA may be exercised against the representative in the Union (LT, SK);
- When SAs order controllers to bring data processing into compliance with the GDPR or decide to impose a fine, the representative should provide SAs with information on the enforcement of these decisions (FR);
- The representative facilitates the exercise of data subjects' rights (BG);
- There is a possibility to enforce investigative and corrective powers on the representative (LU);

- The designation of a representative is crucial because it is not possible to initiate an audit against a controller/processor outside the EEA if there is no representative within the EEA (SE).

2.6.2 Limits to the added value of controller/processor representatives as perceived by SAs

SAs highlighted some limits to the perceived added value of controllers' representatives:

- The possibilities for enforcement against representatives are limited. In line with Recital 80 and Article 27(5) of the GDPR, the designation of a representative in the Union does not affect controllers/processors' responsibility and liability and shall be without prejudice to legal actions that could be initiated against the controller/processor themselves. The GDPR does not establish a substitutive liability of the representative in place of the controller/processor it represents in the Union (cf. EDPB Guidelines, 3/2018) (FI);
- Any possibility to address corrective measures - in particular, administrative fines - to the representative should be further explored, taking into account that it merely 'represents' the Article 3(2) controller/processor (IT).

2.6.3 SAs' experiences of controller/processor representatives

2.6.3.1 Italian SA

To date, the Italian SA has carried out two investigations by contacting the representatives of two companies established in third countries and receiving the cooperation and information it requested.

One case related to a representative designated by a Swiss company in the EEA according to Article 27 of the GDPR. The company processed personal data of Italian data subjects for anti-money laundering purposes. The representative also acts as the company's data protection officer and cooperated fully. The case is ongoing.

Another investigation concerned a Turkish company processing personal data of persons in Italy by means of a website, which designated a representative in the Netherlands. The company granted the data subjects' requests by means of its representative and the case was closed by the Italian SA.

Two ongoing cases relate to controllers under Article 3(2) of the GDPR. They were initiated directly against the controllers as no representatives have been designated (both companies challenge the applicability of the GDPR). The Italian SA notified the controllers, according to Section 166.5 of the Italian Data Protection Code, of the alleged violations, pursuant to the safeguards set out in the Garante's Internal Regulations (cf. also Section 166.9) and are waiting on a reply from the companies. No enforcement actions relating to final decisions of the IT SA have begun.

2.6.3.2 Slovenian SA

The Slovenian SA has initiated one case against an information service provider from the US with a representative in Slovenia. The case is still pending. In the inspection procedure, the SA requested information from the data controller via its representative, and replies were provided in due time.

2.6.4 Legal analysis of the scope of representatives' obligations under the GDPR

The EDPB 3/2018 Guidelines on the territorial scope of the GDPR (Article 3) (version 2.1) highlights the eight following elements that are relevant to the analysis of the scope of representatives' obligations under the GDPR, with respect to the enforcement of SAs' investigative and corrective powers:

- Article 3(2) of the GDPR: data controllers/processors are under the obligation to name a representative in the Union;
- The presence of a representative in the Union does not constitute an 'establishment' for the controller/processor on the basis of Article 3(1) of the GDPR;
- The representative in the Union acts on behalf of the controller/processor it represents with regard to its obligations under the GDPR;
- While not itself responsible for complying with data subject rights, the representative must facilitate communication between data subjects and the controller/processor in order to give effect to the exercise of data subjects' rights;
- The controller/processor's representative shall maintain a record of processing activities under the responsibility of the controller/processor. It is the representative´s own responsibility to be able to provide that record when requested by an SA;
- The representative should perform its tasks according to the mandate received from the controller/processor, including cooperating with the competent SAs on any action taken to ensure compliance with the GDPR. Accordingly, the representative should be able to facilitate any information or procedural exchange between a requesting SA and an Article 3(2) of the GDPR controller/processor. The representative in the Union must therefore be in a position to efficiently communicate with data subjects and cooperate with the SAs concerned;
- The designation of a representative in the Union does not affect the responsibility and liability of the controller/processor under the GDPR and shall be without prejudice to legal actions that could be initiated against the controller/processor themselves;
- The GDPR does not establish substitutive liability of the representative in place of the controller/processor it represents in the Union.

In addition, the EDPB rightly recalls that '(…) *the concept of the representative was introduced with the aim of facilitating the liaison with and ensuring effective enforcement of the GDPR against Article 3(2) of the GDPR controllers/processors. To this end, it was the intention to enable supervisory authorities to initiate enforcement proceedings through the representative designated by the controllers or processors not established in the Union. This includes the possibility for supervisory authorities to address corrective measures or administrative fines and penalties imposed on the controller or processor not established in the Union to the representative, in accordance with articles 58(2) and 83 of the GDPR. The possibility to hold a representative directly liable is however limited to its direct obligations referred to in Article 30 and Article 58(1)a of the GDPR*.'

However, it should be underlined that GDPR Recital 80 specifies *in fine* that '(…) *The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor*.' With respect to this point, Azzi wrote in 2018 that:

> '*There is much controversy as to whether a representative may incur some sort of liability, in addition to the operator, and no guidance has been issued by the Art. 29 WP. Meanwhile, as the first Member State to have implemented the regulation, Germany has interpreted this provision law as enabling civil law proceedings to be directed against the representative. Further, in a recent case against WhatsApp, held under the directive, the Netherlands has considered that the DPO could incur liability in case of non-compliance with the directive, despite this not being specified by the directive. In response, WhatsApp claimed that it could not find any officer ready to endorse such liability, but the "impossibility" argument has been rejected. The Dutch court added that the parties could agree in contract to indemnify the officer in case of liability. Besides, the IAPP, a non-profit organisation which share best practices for privacy management issues, has also interpreted Article 27 of the regulation in this sense: "it seems likely the EU representative would be required to at least initially incur the legal and other costs for addressing enforcement actions and be responsible for paying administrative fines and damage suit awards*".'
>
> '*From those observations and considering the influence that may have the first implementation*

law on other Member States, there is a real possibility for representatives to be subject to enforcement measures. Of course, the law would be more effective if such power of coercion could be exercised locally. Besides, it would reduce the costs inherent to cross-border litigation.'

'*However, a number of objections temper this possibility. First, as it was claimed by WhatsApp, operators might encounter a real difficulty in finding a representative eager to incur a potentially significant liability. Second, a representative may not actually have much influence over the foreign operator and may not have sufficient financial or material means to deal with the sanctions. Finally, even though the obligation to appoint a representative is sanctioned by a fine of up to 2% of the global turnover, there might well be some operators who decide to ignore it and not respond to any sanctions*.'

Millard and Kamarinou (2020) considered that Article 27 did not impose any direct liability on representatives. But they highlighted the wording of Recital 80[67]. They appear to suggest the possibility that Article 27 could be interpreted as allowing SAs to initiate legal proceedings against representatives. With respect to this, they highlight the fact that, e.g, Article 30 of the Spanish Organic Law 3/2018 of 5 December 2018 on the protection of personal data and safeguarding of digital rights provides that:

'1. In the cases in which Regulation (EU) 2016/679 applies to a controller or processor not established in the European Union under Article 3(2) thereof and the processing refers to data subjects found in Spain, the Spanish Data Protection Agency or, where appropriate, the regional data protection authorities, may impose the measures established in Regulation (EU) 2016/679 on the representative, jointly with the controller or processor.

This requirement shall be without prejudice to the liability that could, where appropriate, be borne by the controller or processor and to the exercise by the representative of action under a right of recourse against the relevant party.

2. Moreover, in case of liability in the terms provided for in Article 82 of Regulation (EU) 2016/679, the controllers, processors and representatives shall be jointly liable for the damage caused.'

In a 2021 update, the authors stated that:

'(…) *the EDPB has confirmed that under the GDPR representatives are not liable for infringements of the controller or processor they represent but only for the obligations addressed directly to representatives in Articles 30 and 58(1) of the GDPR. As the nature of the role of representatives is to be a point of contact in the Union for the controller or processor not established in the Union and to facilitate enforcement proceedings against such controllers or processors, it follows that the intention of the GDPR was to "enable supervisory authorities to initiate enforcement proceedings through the representative". In practice, this means that supervisory authorities may "address corrective measures or administrative fines" imposed on controllers or processors not established in the Union to representatives but without holding representatives directly liable for such measures or fines. Representatives act only as a liaison between supervisory authorities and the controllers or processors they represent*.'

It is our current view that, in addition to the EDPB 3/2018 Guidelines regarding the scope of representatives' obligations under the GDPR, it should be considered that:

- SAs should be entitled to send all notifications directed to controllers/processors to the

[67] Millard, Chr. and Kamarinou, D., 'Article 27. Representatives of controllers or processors not established in the Union', in Chr. Kuner, Lee A. Bygrave and Chr. Docksey, *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020, p. 597; the *Update of Selected Articles. Covering developments between 1 August 2019 and 1 January 2021*, May 2021.

representative's physical address in the EU, including orders directed to controllers/processors to appear before SAs' Office or courts. This would mean that there is no need to realise any other sort of notifications notably in the third country where the controller/processor is established;
- Controllers/processors' representatives could be sued by SAs when not acting according to their obligations under the GDPR. This raises the question as to whether it would be possible for SAs to sue representatives for not acting according to their contractual obligations vis-à-vis the controller/processor, as well as the question as to the scope of their liability.

It also raises the question as to whether national legislation could go beyond the GDPR regime in respect of the scope of controllers/processors' representatives' liability.

2.6.5 Key findings

It is clear that the appointment of a controller/processor representative is crucial to the enforcement of SAs' investigative and corrective powers. non-compliance with Article 27 GDPR should be punished under Article 83(4)a of the GDPR (administrative fines).

2.7 INTERNATIONAL COOPERATION FORESEEN IN THE GDPR (ARTICLE 50)

This subsection presents the obstacles that SAs identified in international cooperation in the field of data protection (Section 2.7.1), as well as possible solutions (Section 2.7.2). It also presents SAs' experiences with third countries cooperating on data protection and/or recognising SAs' investigative or corrective powers, and MoUs concluded by some SAs (Sections 2.7.3 and 2.7.4, respectively). It closes with a short consideration of EU trade agreements and the enforcement of SAs' investigative or corrective powers (Section 2.7.5).

2.7.1 Main obstacles to international cooperation in the field of data protection identified by SAs

In their questionnaire responses, SAs identified several obstacles to international cooperation in the field of data protection:

- Differences between national legislations (BG, IT, SK);
- Differences between SAs' procedural regimes (BG, FI, IT, SK);
- Absence of data protection law in third countries (PL);
- General understanding of data protection rules (BG);
- Lack of practice (EE);
- Determining relevant interlocutors in the third country (IT);
- Anonymity of website owners (FI);
- Enforcement of fines/orders (FI);
- Impossibility of producing findings when the data controller is outside the SA's national borders, does not have a website, and refuses to answer SAs' questions or appear for a hearing (FR);
- In exercising their corrective powers, SAs have no way to ensure that the decision would be enforced abroad if the data controller chooses not to comply (FR);
- Under-capacity (small number of employees) (HR);
- Slow pace of administration (HU);
- Probative force of documents collected by another authority in a different jurisdiction (IT);
- Language difficulties (HU, IT);
- Absence of any legally binding and enforceable instrument between public authorities or bodies to establish an effective international cooperation channel and provide guarantees for the transfer of personal data of the complainant to third countries (LU, PL);
- Non-effective (or non-existent) procedures regarding enforcement of the GDPR abroad (PL);

- Non-recognition by the US of European standards on the protection of personal data (in particular, the processing of personal data by US national security protection authorities) (PL).

2.7.2 Tools to improve international cooperation in the field of data protection identified by SAs

SAs identified several tools to improve international cooperation in the field of data protection:

- Stronger international voluntary initiatives, such as the Global Privacy Assembly (BG, FR, LU);
- Guidance with practical examples (EE);
- International agreements in the field of data protection (FI, PL);
- International agreements, MLAT, or administrative arrangements (IT);
- Means to enforce a decision made by an EU SA outside the EU (FR);
- Tools to frame international cooperation (administrative arrangements or international agreements), providing support to the enforcement of SAs decisions and sanctions in third countries and, to the extent possible, to shared investigative actions and appropriate safeguards (FI, FR, IT, PL, SI, PL);
- Issuing of more adequacy decisions (PL);
- Better and more developed communication systems and tools (HR);
- Tools enhancing the pace of administration and supporting translation (HU);
- Ability for several SAs to join a formal request addressed to another SA outside the EU (FR);
- Some cooperation at EDPB level (e.g. template international agreements or administrative arrangements (FR, IT, PL).

2.7.3 Identification of third countries that would cooperate on data protection and/or recognise SAs' investigative or corrective powers

The **French SA** stated that some third countries offer their cooperation depending on whether the offences are recognised in that country. However, they consider it difficult to put in place a formal cooperation considering the different legal frameworks in place. Cooperation with some third countries thus remains informal.

The **Italian SA** and Albanian Data Protection Authority entered into a **Cooperation Agreement** on 10 February 2015. The Agreement envisages joint inspection activities at both public administrative bodies and private entities, including call centres operating in Albania. The underlying objectives include the exchange of experience and know-how, handling of complaints lodged by citizens of either country, provision of support in drafting reports and analyses, and regulatory updates. In 2017, on the basis of this Cooperation Agreement, the **Italian SA** (with a small team of legal and IT experts) participated in an inspection activity by the Albanian Data Protection Authority at two call centres in Albania. This cooperation allowed the Garante to share its expertise on inspection procedures, with a view to fostering enforcement of the Albanian data protection legislation in a sector that often involves processing Italian data subjects' personal data for telemarketing purposes.

2.7.4 MoUs

Some SAs concluded MoUs[68] under the previous EU data protection regime:

- 2012 MoU between the Privacy Commissioner of Canada and the Federal Commissioner for Data Protection and Freedom of Information of **Germany** on mutual assistance in the enforcement of laws protecting personal information in the private sector;
- 2014 MoU between the Privacy Commissioner of Canada and the Data Protection

[68] https://www.priv.gc.ca/en/about-the-opc/what-we-do/memorandums-of-understanding/

Commissioner of **Ireland** on mutual assistance in the enforcement of laws protecting personal information in the private sector;
- 2014 MoU between the Privacy Commissioner of Canada and the College Bescherming Persoonsgegevens (the **Netherlands**) on mutual assistance in the enforcement of laws protecting personal information in the private sector;
- 2014 MoU between the Privacy Commissioner of Canada and the National Supervisory Authority for Personal Data Processing of **Romania** on mutual assistance in the enforcement of laws protecting personal information in the private sector.

2.7.5 Enforcement of SA investigative and corrective powers in EU trade agreements

There are no effective mechanisms for the enforcement of SAs' investigative and corrective powers in the trade agreements concluded by the EU:

- EU-Singapore Free Trade Agreement, 19 October 2018;
- EU-Vietnam FTA, 30 June 2019;
- EU-Canada Comprehensive Economic and Trade Agreement (CETA), 21 September 2019;
- EU-China Comprehensive Agreement on Investment, 30 December 2020;
- EU-UK Trade and Cooperation Agreement, 30 December 2020.

Nor are there such mechanisms in the texts under negotiation:

- EU-Mercosur Trade Agreement;
- EU-Mexico Trade Agreement;
- EU-Australia Trade Agreement;
- EU-New Zealand Trade Agreement[69].

2.7.6 Key findings

Strengthening international cooperation seems the best avenue for better and easier enforcement of SAs' investigative and corrective powers against third-country controllers/processors that fall under the scope of Article 3(2) of the GDPR but are not willing to cooperate with SAs and did not designate an EEA representative. In the short term, the conclusion of MoU (or equivalent) should be considered. The use of legal instruments in the matter of criminal cooperation (e.g. MLAT) could be considered where there is a serious breach of the GDPR that amounts to a criminal offence. Finally, closer cooperation with the EU Commission when the latter is negotiating trade agreements could be useful in creating effective mechanisms to enforce SAs' investigative and corrective powers abroad.

[69] See also the 2016 *Enhanced Partnership and Cooperation Agreement between the European Union and its Member States, of the one part, and the Republic of Kazakhstan, of the other part*, article 237

3 CONCLUSIONS

This Study aimed to analyse the possibilities available to enforce SAs' investigative and corrective powers against third-country controllers/processors that fall under the scope of Article 3(2) of the GDPR but are not willing to cooperate with SAs and did not designate an EEA representative. The analysis focused on controllers and processors established in California (US), the UK, and (to the extent possible) China. The analysis was based on desk research and SAs' responses to a survey of their experience with enforcement in third countries. The main findings of the Study are as follows.

(a) Possibility to summon third-country controllers/processors to appear before SA's Office, or in the SA's national courts or tribunals

SAs do not seem to have the same kind of powers to summon third-country controllers/processors to appear before their Offices or in Courts. We know that Article 58(5) of the GDPR may be used by SAs as soon as the GDPR applies to the controller; however, as SAs must exercise their powers on their national territory, it is not clear whether this precludes SAs initiating legal proceedings in another Member State or in a third country on basis of Article 58(5) of the GDPR. Equally unclear is the position of the CJEU regarding the lack of any kind of establishment of the controller/processor on the territory of any Member State in respect of the possibility to open any 'international jurisdiction or competence' to the benefit of any 'court or tribunal' of the Member State of the SA on the basis of Article 58(5) of the GDPR. In our view, SAs should be entitled to summon a third-country controller/processor that falls within the scope of Article 3(2) GDPR but is unwilling to cooperate with SAs and did not designate an EEA representative to appear before their Office, or in the SA's national courts or tribunals.

(b) Enforcement of SAs' investigative and corrective powers in California, the UK and China

SAs do not qualify as 'courts or tribunals' in the meaning of Article 267 of the TFEU when exercising their investigative and corrective powers, and SAs should be considered to exercise 'public powers' under European law only when making use of special powers that go beyond those arising from the ordinary legal rules applicable to relationships between private individuals. With respect to this, the wording of Article 58 of the GDPR might be slightly misleading as to the nature of these powers (e.g. Article 58(1)c, e, f; Article 58(2)a, b, c, d, e, g). If SAs are not considered to exercise 'public powers' as understood under EU law, there is a possibility that SAs could be considered as acting like 'private persons' in 'civil and commercial matters' (e.g. in the field of international jurisdiction and applicable law). In consequence, the very nature of those powers could have to be additionally ascertained in light of the powers conferred on SAs by their national data protection laws.

In theory, SAs may exercise their investigative and corrective powers in a manner that produces effects beyond the EEA territories within the framework of the relevant international law. However, that does not necessarily imply that:

- Third countries will accept SAs exercising investigative and corrective powers in a manner that produces effects on their territories;
- third countries will accept SAs initiating legal actions or proceedings before their courts or tribunals;
- third countries will recognise that SAs are acting in 'civil or commercial matters' or that they are exercising 'public powers';
- the rules applied by SAs when exercising their investigative and corrective powers are 'acceptable' or 'applicable' in the third countries' courts or tribunals;
- SAs are allowed to send agents abroad to third countries, even with the consent of the controllers/processors established in those countries.

It results from the findings that the enforcement of EU SAs' decisions in California and UK courts may

prove difficult - if not impossible - in a reasonable timeframe and without prejudice to its financial cost. However, the adoption of the California Consumer Privacy Act of 2018 may open the door to active cooperation with the California Privacy Protection Agency. Similarly, cooperation with the UK Data Protection Commissioner seems possible to consider through the prism of Treaty 108+ (Articles 16 and 17), combined with the functions and missions imparted to the UK Commissioner by the UK GDPR and DPA 2018. It is worth noticing that the UK Commissioner has concluded a relatively high number of MoUs with foreign data protection authorities. Cooperation with China seems possible in theory but would require a comprehensive approach, including close cooperation between the EU and the Member State public authorities responsible for the relationship with China. Cooperation with the US through the 2003 MLAT or the US Safe Web Act of 2006 is not impossible but is designed for large criminal cases. Nor is that cooperation limitless or unconditional. Cooperation through the Cloud Act does not seem any simpler.

Effective international cooperation seems to require a similarity of approach and enforcement mechanisms – similar to the traditional notion of reciprocity.

(c) Identification of legal instruments supporting enforcement of SAs' powers

The SAs identified legal instruments that could support enforcement of the GDPR against third-country controllers/processors. The Study highlights some additional instruments that could also usefully be considered.

(d) Sharing SAs' experience and identifying other types of actions

In practice, SAs have some experience of international cooperation, albeit more informally. International cooperation between EU SAs and foreign data protection authorities raises the issue of the appropriate safeguards needed for transferring personal data of data subjects to foreign data protection authorities.

SAs identified some avenues to improve international cooperation in the field of data protection. Direct action on the electronic communications infrastructure or the intermediaries located on the EEA territories (e.g. order to stop collecting personal data or order to shut down websites) seems the most effective.

(e) Possibility to rely on controller/processor unilateral commitments on choice of jurisdiction and applicable law

It seems difficult to effectively rely on commitments from controllers/processors on the choice of jurisdiction or applicable law. However, if SAs are considered to act in 'civil and commercial matters', there could be some room for a degree of choice of jurisdiction and applicable law.

(f) Importance of the appointment of controller/processor representative

The appointment of a controller/processor's representative is crucial to the enforcement of SAs' investigative and corrective powers, even if, ultimately, the representative will not pay for the controller/processor's liability.

(g) Main obstacles to international cooperation in the field of data protection

SAs identified several obstacles to international cooperation in the field of data protection, such as a lack of practice, shortcomings in the legal framework, and problems in producing evidence.

In conclusion, strengthening international cooperation seems to be the best avenue for better and easier enforcement of SAs' investigative and corrective powers against third-country controllers/processors that fall under the scope of Article 3(2) of the GDPR but are not willing to cooperate with SAs and did

not designate an EEA representative.

In the short term, the conclusion of MoUs (or equivalent) should be considered where legally binding instruments (e.g. international agreements, conventions, treaties) cannot quickly be concluded or considered a viable option.

The use of legal instruments in the matter of criminal cooperation (e.g. 2003 MLAT) could be considered where there is a serious breach of the GDPR that amounts to a criminal offence.

Finally, closer cooperation with the EU Commission during the negotiation of trade agreements could be useful in creating effective mechanisms to enforce SAs' investigative and corrective powers abroad.

ANNEX 1 - QUESTIONNAIRE

QUESTIONNAIRE – Information on the legal mechanisms that could help the enforcement of the GDPR against a controller/processor established in the Unites States of America (US), United Kingdom (UK) or China, who falls under its article 3(2).

This questionnaire encompasses a broad range of issues in the difficult matter of enforcing the GDPR against controller/processor established in the US, UK or China but falling under its Article 3(2), and is consecutively divided into 6 parts:

1° Enforcement of SA's Investigating and Corrective Powers against a controller/processor established in the US, UK or China;
2° Identification of legal instruments supporting the enforcement of the GDPR against a controller/processor established in the US, UK or China;
3° Sharing of experience about enforcing the GDPR against a controller/processor established outside the EEA;
4° International cooperation regarding the enforcement of the GDPR against a controller/processor established outside the EEA;
5° The impact of the autonomy of will on the enforcement of the GDPR outside the EEA;
6° Specific questions regarding the enforcement of the GDPR against a controller/processor established outside the EEA.

Please feel free to answer only the questions you are most familiar with.

PART 1. QUESTIONS ABOUT THE ENFORCEMENT OF SAs' INVESTIGATING AND CORRECTIVE POWERS AGAINST A CONTROLLER/PROCESSOR ESTABLISHED IN THE US, UK OR CHINA WHO FALLS UNDER ARTICLE 3(2) OF THE GDPR

1. Please describe the procedure/steps you would follow when exercising your investigating powers against a controller/processor established in the US, UK or China who falls under Article 3(2) of the GDPR and the legal provisions that are applicable for each step?

1.1. If appropriate, please elaborate whether a distinction has to be made between the various investigative powers described in article 58(1) of the GDPR according to their legal nature (administrative act/decision/measure, judicial act/decision/measure, criminal act/decision/investigation, other?):

- Information request
- Data protection audits
- Notification of an alleged infringement
- Access to personal data
- Access to premises

Please use below table to provide your answers:

Type of procedure	Procedural steps in case of information request	Procedural steps in case of data protection audits	Procedural steps in case of notification of an alleged infringement	Procedural steps in case of access to personal data	Procedural steps in case of access to premises
Administrative act/decision/measure					
Judicial act/decision/measure					
Criminal act/decision/investigation					
Other					

1.2. In addition, could explain how you would deal with the issue of the language to be used and indicate the legal basis if any?

2. Could you describe the procedure/steps you would follow when exercising your corrective powers against a controller/processor established in the US, UK or China who falls under Article 3(2) of the GDPR and the legal provisions that are applicable for each step?

2.1. If appropriate, please elaborate whether a distinction has to be made between the various corrective powers described in article 58(2) of the GDPR according to their legal nature (administrative act/decision/measure, judicial act/decision/measure, criminal act/decision/investigation, other?):

- Warning of a possible infringement
- Reprimands
- Order to comply with data subjects' requests to exercise their rights
- Order to comply with the GDPR provisions
- Order to communicate a data breach to the data subject
- Data processing limitation (e.g. ban on processing)
- Order to rectify/erase/restrict processing and notification to recipients
- Withdrawal of a certification
- Administrative fine

- Suspension of data flows to a recipient in a third country or to an international organization

Please use below table to provide your answers:

Type of procedure	Procedural steps in case of warning of a possible infringement	Procedural steps in case of reprimands	Procedural steps in case of order to comply with data subjects' requests	Procedural steps in case of order to comply with the GDPR provisions	Procedural steps in case of order to communicate a data breach to the data subject	Procedural steps in case of data processing limitations	Procedural steps in case of order to rectify/erase/restrict processing and notification	Procedural steps in case of withdrawal of a certification	Procedural steps in case of administrative fine	Procedural steps in case of suspension of data flows to third countries
Administrative act/decision/measure										
Judicial act/decision/measure										
Criminal act/decision/investigation										
Other										

2.2. In addition, could explain how you would deal with the issue of the language to be used and indicate the legal basis if any?

3. Please describe the appropriate safeguards provided for by your national law pursuant to GDPR Article 58(4) (including effective judicial remedy and due process) and that are pertaining when exercising your investigating and corrective powers against a controller/processor established in the US, UK or China who falls under Article 3(2) of the GDPR.

3.1. In addition, please indicate the national legal provisions that are applicable and, if possible, their text in English.

Please use below table to provide your answers:

No.	Appropriate national safeguard and brief description	Legal basis (national legal provision)	English translation
1			
2			
3			

4. Please describe the national legal provisions that are applicable in your country pursuant to GDPR Article 58(5) that allows you as a Supervisory Authority (SA) to bring infringements to the attention of the judicial authorities and to commence or engage otherwise in legal proceedings in order to enforce the GDPR. Please focus on those provisions that are pertaining when you exercise your investigating and corrective powers against a

controller/processor established in the US, UK or China who falls under Article 3(2) of the GDPR.

4.1. In other words, do you have the legal possibility to summon a controller / processor who falls under article 3(2) of the GDPR, to appear in a Court in your country or in front of your office (or in front of any other public institution or body)?
- Yes
- No
- I do not know

4.2. If positive, could you describe such national legal provisions?

In addition:

4.3. Please indicate the legal basis that could open the international jurisdiction of your country to know of a case introduced by you exercising your investigating and corrective powers against a controller/processor who falls under article 3(2) of the GDPR.

4.4. Please indicate the law that would be applied to the controller/processor who falls under article 3(2) of the GDPR (beyond the application of the GDPR rules) (and the legal reasoning for applying a foreign legislation).

5. Please describe any additional powers provided by your national law that could be pertaining when exercising your investigating and corrective powers against a controller/processor established in the US, UK or China who falls under Article 3(2) of the GDPR.

PART 2. IDENTIFICATION OF THE LEGAL INSTRUMENTS SUPPORTING THE ENFORCEMENT OF THE GDPR AGAINST A CONTROLLER/PROCESSOR ESTABLISHED IN THE US, UK OR CHINA WHO FALLS UNDER ITS ARTICLE 3(2)

1. Please list and describe the national, European and international legal instruments you could rely on when enforcing the GDPR against a controller/processor established in the US, UK or China who falls under its Article 3(2), in the matter of Cooperation / Assistance / Act or Decision Notification / Act or Decision Recognition / Direct or Indirect Enforcement.

In addition:

1.1. Please indicate whether these legal instruments are applicable in all matters (including data protection) or are specific to data protection.

1.2. Please specify the nature of these legal instruments (International Agreement, Treaty, Convention, Informal Agreement, Bilateral Agreement, (including Memorandum of Understanding), etc.).

1.3. If possible, please provide an English version of the text.

Please use the following table to provide your answers:

No	Name of the legal instrument	Geographical coverage (national, EU, international,	Coverage (Cooperation / Assistance / Act or Decision Notification / Act or Decision Recognition / Direct or Indirect Enforcement / All)	Is this instrument data protection specific? (Yes/No/N/A)	Nature of the legal instrument (International Agreement, Treaty, Convention, Information Agreement, Bilateral Agreement, other)	Link to the agreement (in English if possible)
1						
2						
3						
4						
5						

1.4. Please indicate any discussion or work on the issue of the international cooperation in the field of data protection that are ongoing at the moment in your country (cooperation, mutual assistance, engagement of stakeholders, promotion of exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries).

PART 3. SHARING OF EXPERIENCE AND THOUGHTS ABOUT THE ENFORCEMENT OF THE GDPR AND THE SAS' INVESTIGATING AND CORRECTIVE POWERS AGAINST A CONTROLLER/PROCESSOR ESTABLISHED OUTSIDE THE EEA BUT WHO FALLS UNDER ARTICLE 3(2) OF THE GDPR

This part of the questionnaire aims at collecting your experience and reflections on the enforcement of the GDPR and the SAs' investigating and corrective powers against a controller/processor established outside the EEA but who falls under Article 3(2) of the GDPR.

1. **Please describe any experience (even by another SA) or knowledge that you have in the matter of enforcing SAs' investigating and corrective powers abroad (beyond the EEA zone; meaning, directly on the territory of a third country where the controller/processor is located). Examples of such experience could include sending an auditing or investigating teams abroad etc.**

1.1. If possible, please provide a brief account of the case(s) (facts, legal reasoning and results) and a copy of the decision in English.

In addition:

1.2. Do you have any knowledge of a country outside the EEA zone that would offer its cooperation in the field of data protection and/or would recognize your investigative or corrective powers?
- Yes
- No
- I do not know

1.3. If positive, could you elaborate on the legal framework of this international cooperation?

1.4. Could you describe the external resources and legal support at your disposal at national, European or international level, in order to help and support you when enforcing the GDPR against a controller/processor who falls under article 3(2) of the GDPR (e.g. support from Ministry of Justice or Foreign Affairs, or from any other public institution or body)?

1.5. What additional help or support could be useful in your view?

2. **Have you heard of any application of the Principle of International Courtesy in the field of data protection in your country or in another country?**
- Yes
- No
- I am not familiar with this principle

2.1. If positive, could you elaborate on the case (facts, legal reasoning and results)?

3. **Please describe any experience in which you have received a request/demand of international cooperation/assistance/enforcement in the field of data protection from a foreign non-European data protection authority (located outside the EEA zone) (or from any other foreign non-European public institution or body acting in the field of data protection)?**

3.1. In addition, please describe the procedure and steps when enforcing a foreign decision (from outside the EEA zone) in the field of data protection in your country with the indication of the legal basis.

4. **In your view, what is the added value of the designation of a representative in the EEA in accordance with Art. 27 GDPR in case of enforcement? Have you ever initiated a case against such a representative (located in your country) of a controller/processor who falls under Article 3(2) of the GDPR? If positive, could you elaborate and describe the case (facts, legal reasoning and results)?**

5. **In your view, what other types of actions could be taken in the EEA to ensure enforcement of the GDPR relating to processing taking place by controllers or processors established in third countries (e.g. order to stop collecting/processing personal data by means of a website)?** Please explain why.

PART 4. QUESTIONS ABOUT INTERNATIONAL COOPERATION AND ASSISTANCE IN THE MATTER OF ENFORCING THE GDPR AGAINST A CONTROLLER/PROCESSOR ESTABLISHED OUTSIDE THE EEA BUT WHO FALLS UNDER ITS ARTICLE 3(2)

1. **What are the national legal provisions applicable in your country when a European SA requests your assistance or your cooperation in the field of data protection? Could you describe the procedure?**

2. **In your view, what are the main obstacles to the international cooperation in the field of data protection?**

3. **In your view, what are or what could be useful tools to improve the international cooperation in the field of data protection?**

3.1. In addition, please elaborate if you think it could be useful to formalize further the cooperation in this respect at the level of the EDPB?

PART 5. QUESTIONS ABOUT THE POSSIBILITY FOR THE AUTONOMY OF WILL TO IMPACT THE ENFORCEMENT OF THE GDPR AGAINST A CONTROLLER/PROCESSOR ESTABLISHED IN THE US, UK OR CHINA WHO FALLS UNDER ITS ARTICLE 3(2)

This part of the questionnaire focuses on the possibility to recognize the impact of controller/processor's contractual or unilateral commitments in the matter of enforcing GDPR obligations.

1. **Are you able to conclude an agreement with the controller / processor who falls under article 3(2) of the GDPR in order to choose a jurisdiction to which to submit their dispute?**
   - Yes
   - No
   - I do not know

1.1. If positive, could you elaborate on the legal reasoning?

In addition:

1.2. Can you rely on a choice of jurisdiction contained in the Binding Corporate Rules?
- Yes
- No
- I do not know

1.3. If positive, could you elaborate on the legal reasoning?

1.4. Can you rely on a choice of jurisdiction contained in a unilateral commitment from the controller/processor?
- Yes
- No
- I do not know

1.5. If positive, could you elaborate on the legal reasoning?

2. **Can you conclude an agreement with the controller / processor who falls under article 3(2) of the GDPR in order to choose the applicable law to their dispute?**
   - Yes
   - No
   - I do not know

2.1. If positive, could you elaborate on the legal reasoning?

In addition:

2.2. Can you rely on a choice of applicable law contained in Binding Corporate Rules?
- Yes
- No
- I do not know

2.3. If positive, could you elaborate on the legal reasoning?

2.4. Can you rely on a choice of applicable law contained in a unilateral commitment from the controller/processor?

- Yes
- No
- I do not know

2.5. If positive, could you elaborate on the legal reasoning?

PART 6. SPECIAL QUESTIONS REGARDING THE ENFORCEMENT OF THE GDPR AGAINST A CONTROLLER/PROCESSOR ESTABLISHED OUTSIDE THE EEA BUT WHO FALLS UNDER ITS ARTICLE 3(2)

This last part of the questionnaire concerns very specific topics in the area of enforcing the GDPR against a controller/processor established outside the EEA but who falls under its article 3(2).

1. **Could the courts in your country or any other national public institution or body review the acts and decisions from a foreign (non-European) data protection authority (located outside the EEA)?**
   - Yes
   - No
   - I do not know

1.1. If positive, could you elaborate on the legal reasoning?

2. **Could the courts in your country or any other national public institution or body enforce the acts and decisions from a foreign data protection authority (located outside the EEA)?**
   - Yes
   - No
   - I do not know

2.1. If positive, could you elaborate on the legal reasoning?

3. **What is the probative force attached to the acts and decisions of a foreign data protection authority (located outside the EEA) in your country? Could you elaborate on the legal reasoning and indicate the legal basis?**

Thank you!

ANNEX 2 – SOURCES OF INFORMATION

I. International conventions and agreements

1. 1971 Hague Convention on the recognition and enforcement of foreign judgments in civil and commercial matters.
2. 2001 Agreement between the Government of Ireland and the Government of the Hong Kong Special Administrative Region of the People's Republic of China concerning mutual legal assistance in criminal matters (Treaty Series 2012, n° 2).
3. 2001 US and Republic of Ireland Agreement relating to mutual legal assistance in criminal matters.
4. 2003 Agreement on mutual legal assistance between the European Union and the United States of America (2003 MLAT).
5. 2005 Hague Convention on choice of court agreements.
6. 2007 Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Lugano Convention).
7. 2009 Agreement between the European Union and Japan on mutual legal assistance in criminal matters.
8. 2016 Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences.
9. 2019 Hague Convention on the recognition and enforcement of foreign judgments in civil or commercial matters.

II. Council of Europe conventions

1. 1959 Convention on Mutual Assistance in Criminal Matters (ETS n° 30).
2. 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (now Treaty 108+).
3. 2001 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows.

III. EU law and documents

<u>Fundamental texts of the EU</u>

1. Charter of Fundamental Rights of the European Union.
2. Treaty on the Functioning of the European Union (consolidated version).

<u>EU directives and regulations</u>

1. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
2. Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty.
3. Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I).
4. Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.
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).
6. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.
7. Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC.
8. 2021 Decision on the adequate protection of personal data by the United Kingdom (General Data Protection Regulation, GDPR).
9. 2021 Decision on the adequate protection of personal data by the United Kingdom (Law Enforcement Directive).

EDPB guidelines and other EU documents

1. Brief of the European Commission on behalf of the European Union as Amicus Curiae in support of neither party – United States of America v. Microsoft Corporation (US Court of Appeals, 2e Circuit), n° 17-2.
2. EDPB 3/2018 Guidelines on the territorial scope of the GDPR (Article 3) (version 2.1).
3. Final Report on 'Data protection in the judiciary: the concept of courts/judicial authorities acting in their judicial capacities', EDPS/2019/02-01, 2020.

Existing EU trade agreements:

1. EU-Singapore Free Trade Agreement, 19 October 2018.
2. EU-Vietnam FTA, 30 June 2019.
3. EU-Canada Comprehensive Economic and Trade Agreement (CETA), 21 September 2019.
4. EU-China Comprehensive Agreement on Investment, 30 December 2020.
5. EU-UK Trade and Cooperation Agreement, 30 December 2020.
6. 2016 Enhanced Partnership and Cooperation Agreement between the European Union and its Member States, of the one part, and the Republic of Kazakhstan, of the other part, 2016.

EU trade agreements under negotiation:

1. EU-Mercosur Trade Agreement.
2. EU-Mexico Trade Agreement.
3. EU-Australia Trade Agreement.
4. EU-New Zealand Trade Agreement.

IV. US law

Federal Law:

1. Revised version of the 1962 Uniform Foreign-Country Money Judgments Recognition Act
2. US Code, Title 18, Chapter 119, Section 2511(2)(j).
3. Undertaking Spam, Spyware, and Fraud Enforcement With Enforcers beyond Borders Act of 2006 (US Safe Web Act of 2006).
4. 2018 Clarifying Lawful Overseas Use of Data Act' (Cloud Act).
5. FTC, Office of International Affairs, US Safe Web Act Information Sheet.

California law:

1. State of California, Civil Code, Division 3. Obligations. Part 4. Obligations arising from particular transactions. Title 1.81.5. California Consumer Privacy Act of 2018, § 1789.199.10.
2. California Code of Civil Procedure (CCP), Part 3. Of Special Proceedings of a Civil Nature, Title 11. Money Judgments of other jurisdictions, Chapter 2. Foreign-Country Money Judgments, §§1713-1725.
3. California Consumer Privacy Act of 2018.

V. UK law

1. Foreign Judgments (Reciprocal Enforcement) Act 1933.
2. UK Data Protection Act 2018 (DPA 2018).
3. UK GDPR.

VI. China law

1. 2021 Personal Information Protection Law (PIPL).
2. 2021 Data Security Law.

VII. Case-law

US case-law:

1. United States Court of Appeals, Yahoo! Inc. v. *La Ligue contre le racisme et l'antisémitisme et l'Union des étudiants juifs de France*, 433 F.3d 1199, 1202 (9th Cir. 2006) (en banc).
2. United States District Court, Hugo Elliot v. PubMatic Inc., Case 4:21-cv-01497-PJH (Northern District of California 2021).

CJEU case-law:

1. CJEU (Grand Chamber), 6 September 2017, C-413/14, *Intel Corp. v European Commission*.
2. CJEU (3d ch.), 3 October 2019, C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*.
3. CJEU (3d ch.), 9 July 2020, C-272/19, *VQ v Land Hessen*.
4. CJEU, 16 July 2020, C-73/19, *Belgische Staat v Movic BV, Events Belgium BV, Leisure Tickets & Activities International BV*.
5. CJEU (Grand Chamber), 15 June 2021, C-645/19, Facebook Ireland Limited, Facebook Inc., *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit*.

VIII. MoU (or equivalent)

1. 2012 MoU between the Privacy Commissioner of Canada and the Federal Commissioner for Data Protection and Freedom of Information of Germany on mutual assistance in the enforcement of laws protecting personal information in the private sector.
2. 2013 MoU between the United States Federal Trade Commission and the Office of the Data Protection Commissioner of Ireland on mutual assistance in the enforcement of laws protecting personal information in the private sector.
3. 2014 MoU between the Privacy Commissioner of Canada and the Data Protection Commissioner of Ireland on mutual assistance in the enforcement of laws protecting personal information in the private sector.
4. 2014 MoU between the Privacy Commissioner of Canada and the College Bescherming Persoonsgegevens (the Netherlands) on mutual assistance in the enforcement of laws protecting personal information in the private sector.
5. 2014 MoU between the Privacy Commissioner of Canada and the National Supervisory Authority for Personal Data Processing of Romania on mutual assistance in the enforcement of

laws protecting personal information in the private sector.
6. 2015 Cooperation Agreement between the Italian SA and the Albanian Data Protection Authority.
7. 2015 MoU between the United States Federal Trade Commission and the Dutch Protection Authority on mutual assistance in the enforcement of laws protecting personal information in the private sector.
8. 2019 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and Canadian Radio-television and Telecommunications Commission for cooperation in the enforcement of laws protecting personal data.
9. 2019 MoU between the Personal Data Protection Commission of the Republic of Singapore and the Information Commissioner for the United Kingdom for cooperation in the enforcement of laws protecting personal data.
10. 2020 US Federal Trade Commission and UK ICO MoU on mutual assistance in the enforcement of laws protecting personal information in the private sector.
11. 2020 MoU between the Privacy Commissioner of Canada and the Information Commissioner of the United Kingdom on mutual assistance in the enforcement of laws protecting personal information in the private sector.
12. 2020 MoU between the Privacy Commissioner for Personal Data of Hong-Kong, China and the Information Commissioner for the United Kingdom for cooperation in protecting personal data.
13. 2020 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and the New Zealand Department of Internal Affairs for cooperation in the regulation of unsolicited electronic messages.
14. 2020 MoU between the Information Commissioner and the Global Cyber Alliance.
15. 2021 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and the Office of the Privacy Commissioner for New Zealand for cooperation in the enforcement of laws protecting personal data.
16. 2021 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and the National Privacy Commission of the Philippines for cooperation in the regulation of laws protecting personal data.

IX. OECD documents

1. 2007 Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy.
2. 2012 Background Note on Improving International Co-operation in Cartel Investigation, DAF/COMP/GF(2012)6).
3. 2020 Summary of Discussion 'Roundtable on Legislative Initiatives to Improve Cross-border Enforcement Cooperation', DSTI/CP(2019)21/FINAL.

X. Other international documents

1. International Conference of Data Protection and Privacy Commissioners (ICDPPC), Global Cross-border Enforcement Cooperation Agreement, version 17, 2017.
2. Global Privacy Enforcement Network (GPEN), Action Plan for the Global Privacy Enforcement Network, 2013.
3. APEC, Cross-border Privacy Enforcement Arrangement (CPEA) (2019 version).

XI. Legal literature

Papers:

1. Azzi, A., 'The challenges faced by the extraterritorial scope of the General Data Protection Regulation', *Journal of Intellectual Property, Information Technology and e-Commerce Law*, Vol. 9, No. 2, 2018, p. 59.

2. Browne, O. and Watret, T., *Enforcement of foreign judgments*, 10th ed., London, Law Business Research, Lexology, 2020.
3. Cassart, A., 'Premières réflexions sur le Cloud act: contexte, mécanismes et articulations avec le RGPD', Bruxelles, Larcier, *Revue du droit des technologies de l'information*, Vol. 73, 2018.
4. Chivvis, M., 'Reexamining the Yahoo! litigations: toward an effects test for determining international cyberspace jurisdiction', *University of San Francisco Law Review*, 2007, Vol. 41, p. 699.
5. Dorwart, H., Zanfir-Fortuna, G. and Girot, Cl., 'China's new comprehensive data protection law: context, stated objectives, key provisions', *Future of Privacy Forum*, 20 August 2021.
6. Elkind, D., *L'efficacité des décisions administratives étrangères dans l'Union européenne : Etude de droit administratif transnational*, Université de Bordeaux, 2018.
7. Freyria, Ch., 'La notion de conflit de lois en droit public', in *Travaux du Comité français de droit international privé*, 1962-1964, pp. 106-107.
8. Idot, L., '"*La matière civile et commerciale" à l'épreuve de l'intervention du Ministre de l'Economie en droit de la consommation'*, note sous CJUE (1e ch.), 16 Juillet 2020, aff. C-73/19, Paris, Dalloz, *Revue critique de droit international privé*, Vol. 2, No. 15, 2021, p. 383, 394.

Books and book chapters:

1. Bradley, C.A., *International Law in the U.S. Legal System*, 3d ed., Oxford University Press, 2021.
2. Cheshire, North & Fawcett, *Private International Law*, 15th ed., Oxford University Press, 2017.
3. Folsom, R., *Principles of International Litigation and Arbitration*, 2d ed., West Academic, Concise Hornbook, 2019.
4. Greenleaf, G., *Asian Data Privacy Laws. Trade and Human Rights Perspectives*, Oxford University Press, 2017.
5. Hay, P., Borchers, P.J., Symeonides, S.C. and Whytock, Chr. A., *Conflict of Laws*, 6th ed., West Academic, Hornbook Series, 2018.
6. Millard, Chr. and Kamarinou, D., 'Article 27. Representatives of controllers or processors not established in the Union', in Chr. Kuner, Lee A. Bygrave and Chr. Docksey, *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020, p. 597 (update of selected articles, covering developments between 1 August 2019 and 1 January 2021, May 2021).
7. Rustad, M., *Global Internet Law*, 3d ed., West Academic, Hornbook Series, 2020, pp. 182-183.
8. Spillenger, Cl., *Principles of Conflict of Laws*, 3d ed., West Academic, Hornbook Series, 2020.

ANNEX 3 - ACRONYMS AND ABBREVIATIONS

The table provides a preliminary list of acronyms and abbreviations used throughout this Study.

Acronyms and Abbreviations	Meaning
APEC	Asia-Pacific Economic Cooperation
BCR	Binding Corporate Rules
BG	Bulgaria
Charter	Charter of Fundamental Rights of the European Union
CAC	Cyberspace Administration of China
CiPL	Chinese Civil Procedure Law
CJEU	Court of Justice of the European Union
CNIL	*Commission nationale de l'informatique et des libertés*
CZ	Czechia
DE	Germany
DPA	Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information
DPA 2018	UK Data Protection Act
DK	Denmark
ECHR	European Convention on Human Rights
EE	Estonia
EEA	European Economic Area
EEA representative	Controller/processor's representative in the EEA or the EU
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ES	Spain
EU	European Union
FI	Finland
FR	France
FTC	US Federal Trade Commission
GPA	Global Privacy Assembly
GPEN	Global Privacy Enforcement Network
GDPR	General Data Protection Regulation
HR	Croatia
HU	Hungary
ICDPPC	International Conference of Data Protection and Privacy Commissioners
ICO	Information Commissioner's Office or the UK Data Protection Commissioner
IS	Iceland
IT	Italy
LED	Law Enforcement Directive
LT	Lithuania
LU	Luxembourg
MLAT	Mutual Legal Assistance Treaty
MoU	Memorandum of Understanding
OECD	Organisation for Economic Co-operation and Development
PDPA	Bulgarian Personal Data Protection Act
PIPL	Chinese Personal Information Protection Law
PL	Poland
SA	Supervisory Authority
SDPI	Lithuanian State Data Protection Inspectorate
SE	Sweden
SI	Slovenia

Acronyms and Abbreviations	Meaning
SK	Slovakia
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom
UK GDPR	UK General Data Protection Regulation
UK	United Kingdom
US	United States of America