EU's One-Stop-Shop Mechanism: Thinking Transnational

Andra Giurgiu, Gertjan Boulet and **Paul De Hert** discuss the form of One-Stop-Shop and the role of the different actors.

A company conducting business in more than one EU country that involves the processing of personal data had, so far, to deal and comply with the rules of various national data protection authorities (DPAs). The implementation of Directive 95/46/EC[1] by member states left room for different national data protection frameworks. Due to the existing national specifics, this legal fragmentation makes compliance with data protection rules quite burdensome for companies that conduct business in the Union. At the same time, data subjects face the challenge of enforcing their rights, especially against companies located in another member state. The proposed General Data Protection Regulation (GDPR)[2] with its direct applicability should help to overcome these problems and harmonise and consolidate the EU's Single Market.

One of the means of strengthening EU data protection law for consumers and for businesses is through the so-called "One-Stop-Shop". This mechanism sets up a single contact point whereby companies doing business in more than one EU member state will have to deal with only one DPA, namely that of the member state of their main establishment. At the same time, the One-Stop-Shop would put consumers in a better position to enforce their rights against such companies.

When does the One-Stop-Shop apply?

The main idea of the One-Stop-Shop is that of "streamlining procedures and allocating competences among DPAs"[3] in so-called "transnational cases"[4]. Therefore, matters having an impact in more than one member state shall be dealt with under the One-Stop-Shop mechanism whereas matters of a purely local impact should be handled by the local DPA. But this distinction might not always be so easy to make.

In essence, the One-Stop-Shop applies to two scenarios.[5] The first scenario ("multiple establishments scenario") refers to the situation when a company has several establishments (at least two) in the EU.[6] A second scenario ("affected data subjects scenario") is when a company has just one establishment in the EU and when personal data of residents of at least one other member state are processed.[7] In practice, a combination of the two scenarios could also be possible.

An establishment in the EU seems to be the precondition for the application of the One-Stop-Shop.[8] It is not clear though how to deal with cases where there is no establishment in the EU but when personal data of EU residents of several member states are processed and the GDPR would be applicable on the grounds of article 3 paragraph 2 – in line with the enlarged territorial scope of application of the Regulation[9] – because the company is offering goods or services to data subjects in several EU member states or it is monitoring their behaviour. It seems that in the absence of such an establishment, the cooperation between DPAs and the consistency mechanisms discussed below will have to play an important role.

Which DPA is competent?

For the first "multiple establishments scenario" the competence as a "lead" authority under the One-Stop-Shop belongs to the DPA of the country of the main establishment[10] of that company. In the "affected data subjects scenario", the lead DPA will be determined according to the place of the single establishment of the company. In case of a combination of the two scenarios, we would argue that the competence as a lead DPA will remain with the DPA of the member state of the main establishment of that company. The DPAs of the other establishments or of the member states where the data subjects reside are considered to be "concerned" DPAs and thus part of the One-Stop-Shop mechanism.

Supposing a company has establishments in Germany, Italy and France and its main establishment is in Italy, the Italian DPA will act as lead DPA and the German and France DPAs will be considered "concerned" DPAs[11]. The German and French DPAs can be considered "concerned" by the processing because the company has an establishment on their territory, because the data subjects whose personal data is processed' reside on their territory or because of an underlying complaint that has been lodged with them.

What are the powers of DPAs under the One-Stop-Shop?

As a general rule, each DPA is competent on its own territory being invested with powers of investigation, intervention and advisory powers as well as powers to hear claims and engage in legal proceedings[12]. The One-Stop-Shop has complemented the general competence of DPAs on their own territory by the new competence as a lead authority for companies established in several member states. It thus calls into question the division of powers between DPAs and the issue of cooperation between them, particularly with regard to the question of which powers shall be exercised by the local DPA and which by the lead DPA. It has been debated whether the competence of the lead DPA should be exclusive or not and whether this exclusivity should concern all or only some of the powers it is invested with. The Council[13] proposed a new division of powers of national DPAs grouped into the following categories: investigative powers, corrective powers, authorisation and advisory powers. Discussions have focused on the authorisation and corrective

powers of DPAs and whether the lead DPA should have exclusive competence with regard to these powers. It is the measures producing legal effects in several member states, resulting from the authorisation and corrective powers of DPAs, such as imposing an administrative fine[14] for example or authorising transfers to third countries, which raise issues of whether the lead DPA should have the last word or be forced to take into account diverging opinions of other DPAs and ultimately submit the matter to the consistency mechanism discussed below. In the view of the European Data Protection Supervisor, "the role of a lead authority should not be seen as an exclusive competence, but rather as a structured way of cooperation with other competent supervisory authorities, as the 'lead authority' will depend heavily on the input and support of other supervisory authorities at different points in the process".[15]

In the end, a DPA cannot take a decision – especially on a measure having legal effects such as imposing sanctions – which is directly and necessarily binding in other countries. In an Opinion in a case before the Court of Justice of the European Union[16] (p.1) the Advocate General concluded – under the provisions of Directive 95/46/CE – in a similar matter.[17] The starting point of his reasoning is that, in line with article 28 paragraph 6 of the Directive, a DPA is competent, irrespective of the national law applicable to the processing in question, to exercise, on the territory of its own Member State, all the powers it is invested with. The Advocate General argued however that a DPA – although having the competence to monitor processing activities on its own territory to which the law of another member state applies – does not have the competence to impose sanctions in relation to those processing activities. According to the Advocate General, the competence to impose sanctions in this case belongs to the DPA of the member state the law of which is applicable to the processing activities in question. The Advocate General considers that a different interpretation would be incompatible with the principles of legality and national sovereignty.[18]

Contrary to the current situation, under the GDPR a DPA will also be able to apply its national law when a data subject on its territory lodges a complaint in relation to processing activities by a company not established on that territory. It is therefore to be seen if, and to what extent, this additional jurisdictional ground under the GPDR, which is responsive to data subject rights, will also entail sanctioning powers for the same DPA. The same question may be asked when a lead DPA, which can apply its national law by definition, has to deal with a case regarding processing activities by companies on its territory, but in relation to data subjects in other countries.

> The future EDPB is meant to replace the current Article 29 Working Party.

The consistency mechanism and European DP Board

To fully understand the One-Stop-Shop mechanism it is necessary to explore other novelties proposed in the GDPR, in particular the consistency mechanism and the European Data Protection Board (EDPB). The main rationale behind the consistency mechanism is to set up a clear procedure for the cooperation of DPAs and to guarantee a uniform approach when a measure has an impact in several member states. The proposed Regulation determines a set of cases when this mechanism would apply, such as the adoption of Binding Corporate Rules.[19] But consistency can also be triggered as a result of "unsuccessful cooperation" between the DPAs (or between DPAs and the EDPB) under the One-Stop-Shop, where there are divergent views and a common agreement cannot be reached. The GDPR also provides for an urgency procedure derogating from the need to submit a matter to the consistency mechanism for exceptional circumstances when a DPA considers it urgent to act so as to protect the rights of the data subjects.[20] The consistency mechanism is finalised with an opinion of the EDPB, which also plays the role of a dispute resolution body in case of conflicts between the DPAs.

The future EDPB is meant to replace the current Article 29 Working Party. It shall be composed of the head of one supervisory authority of each member state and of the European Data Protection Supervisor and have the role of ensuring the consistent application of the proposed Regulation. Whether it should be granted legal personality or not[21] and whether its decisions should be binding[22] are matters still disputed and will have to be settled during the current Trilogue. The Commission does not propose giving binding powers to the EDPB. The Parliament introduces very limited binding powers where there is a disagreement between the EDPB and the lead authority. The Council expands the binding powers to cases of conflict resolution between DPAs or between DPAs and the EDPB and for some transnational matters which affect more than one member state.

Conclusion

The forthcoming GDPR will introduce a mandatory One-Stop-Shop mechanism as a welcome innovation in the EU data protection legal framework. Based on the practice of the BCRs developed in the past years[23], this mechanism is not unique to data protection but exists also in other areas of law. Although much seems to have been clarified in the draft GDPR, some questions are still open. The exact scope of the One-Stop-Shop, the material competence of the lead DPA or the issue of conferring binding powers to the EDPB are matters which will have to be settled before the end of the Trilogue. But even after the adoption of the Regulation, the practicality and efficiency of the One-Stop-Shop will still need to prove themselves.

The One-Stop-Shop is the result of the clear choice not to create one single EU data protection agency which would centralise the current decentralised structure of data

protection supervision and not necessarily ease the progress of decision making.[24] The proposed system relies on national agencies, set up according to national laws, that are proposed to work together to make European law possible. It is self-evident that this systems needs to be scrutinised in the future to see whether it works and that other regulatory options are kept open in case the answer is 'no'. The yardstick should not only be the 'service' offered to companies to 'shop only once', but also the ease for data subjects to find an effective remedy when confronted with problems caused by international players. The double concern for a flexible internal market and the idea of access to justice will need to guide further policy-making.

AUTHORS

Andra Giurgiu is Researcher (Postdoc) at the Interdisciplinary Center for Security, Reliability and Trust, University of Luxembourg. Gertjan Boulet is Ph.D. candidate at the Vrije Universiteit Brussel and visiting scholar at Korea University. Paul De Hert is Professor at the Vrije Universiteit Brussel and at Tilburg University.
Emails: andra.giurgiu@uni.lu
gertjan.boulet@vub.ac.be
paul.de.hert@uvt.nl

REFERENCES

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995, 0031 – 0050.
2 The General Data Protection Regulation was proposed by the European Commission on the 25th of January 2012. After going through more than 3000 amendments the European Parliament gave its voted in March 2014. In June 2015 the Council also managed to reach a common position. Now a so-called "Trilogue" has started where the institutions need to agree on a common text so that the final text can be adopted. This is hoped to happen by the end of this year, beginning of the next. It would still take two more years though before the Regulation comes into force.
3 A. Galetta, P. De Hert, The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-oriented Remedial System?, in Review of European Administrative Law; vol 8, no.1, 125-151.
4 Definition of the concept "transnational" can be found in art. 4 parag. 19b of the Council text of June 2015.
5 Whereas the first scenario seems to be undisputed among all three institutions, the second one, was not initially included in the Commission text, but introduced by the Parliament and appropriated also by the Council - see definition of "transnational processing" in art. 4 parag. 19b Council common text of June 2015.
6 Art. 51 parag. 2 of the Commission Proposal of January 2012 states that "Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation."
7 Art. 54a Parliament common text of March 2014 states that " Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, or where personal data of the residents of several Member States are processed, the supervisory authority of the main establishment of the controller or processor shall act as the lead authority responsible for the supervision of the processing activities of the controller or the processor in all Member States, in accordance with the provisions of Chapter VII of this Regulation."
8 As well as the general condition that the processing takes place in the context of the activities of that (those) establishment(s).
9 The Commission's Proposal foresees in art. 3 parag. 2 an enlarged scope of application of EU data protection rules to situations when a company does not haven an establishment in the EU but processes personal data of data subjects residing in the Union, where such processing relates to " the offering of goods or services to such data subjects in the Union" or to "the monitoring of their behaviour".
10 According to art.4 parag. 13 of the Commission Proposal, the main establishment of a controller is the place where the main decisions are taken as regards "the purposes, conditions and means of the processing of personal data". For the processor the main establishment is the "place of its central administration in the Union". The proposal also states in recital 27 that the main establishment shall be determined by objective criteria, which take into account the effective and real exercise of management activities. Bottom line is that the place where the real power is exercised from should be considered as main establishment.
11 See definition of "concerned DPA" in art. 4 parag. 19a Council common text of June 2015.
12 Directive 95/46/CE in art. 28, see also FRA study Data Protection in the European Union: the role of National Data Protection Authorities, 2010, pp.20-28.
13 Art. 53 Council common text of June 2015.
14 The Regulation also levels the powers of the DPAs and strengthens them by investing DPAs with the power to impose administrative sanctions on controllers in the form of high fines going up to 2% (Commission and Council) or even 5% (Parliament) of its annual worldwide turnover.
15 Opinion of the European Data Protection Supervisor on the data protection reform package of 7 March 2012, point 217, p.39.
16 CJEU, Advocate General Opinion of 25 June 2015 in case C-230/14, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság hatóság, CJEU Judgment given on 1 October 2015.
17 See *Privacy Laws & Business International Report*, Issue 136, August 2015, p.5.
18 See point 66 of the above mentioned Opinion.
19 However the Commission or any DPA can request that a matter should be dealt with under this mechanism.
20 Art. 61 Commission text of January 2012.
21 According to art. 64 parag. 1a Council text of June 2015 the EDPB should have legal personality.
22 See especially art. 58a parag.7 Parliament text of March 2014 and art. 57 parag. 3a and art. 68 parag. 1 of the Council text of June 2015.
23 See WP29, Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules, adopted on 24 June 2008 introducing key notions such as 'lead authority'.
24 It seems that the alternative of creating an EU body with legal personality which should play the role of the One-Stop-Shop has also been discussed. See Letter of the European Data Protection Supervisor to the Presidency of the Council of the European Union, of 14 February 2014 with regard to the Progress on the data protection reform package, p.4.

