CNIL's Decision Fining Google Violates One-Stop-Shop

Lokke Moerel

TILT, Tilburg University, The Netherlands
e.m.l.moerel@uvt.nl

TILT Law & Technology Working Paper No. 002/2019
19 February 2019, Version: 1.0

This paper can be downloaded without charge from the Social Science Research Network Electronic Paper Collection
http://ssrn.com/abstract=3337478

An overview of the TILT Law & Technology Working Paper Series can be found at:
http://www.tilburguniversity.nl/faculties/law/research/tilt/publications/workingpapers/
THE CNIL’S DECISION IMPOSING A FINE ON GOOGLE

On 21 January 2019, the French Data Protection Supervisory Authority (CNIL) imposed a penalty of 50 million euros on Google. In its assessment, the CNIL considered itself competent to rule on complaints filed in France alleging unlawful processing of personal data by Google. The decision was made despite the fact that the complaints concerned a cross-border processing in the EU, in respect of which the General Data Protection Regulation (GDPR) provides for a one-stop-shop enforcement mechanism (ISS) by the supervisory authority (SA) of the ‘main establishment’ of a company in the EU. In its decision, the CNIL considered that Google does have EU headquarters in Ireland, but that this Irish entity ‘did not have a decision-making power’ in relation to the relevant cross-border data processing activities to which the complaints related. For that reason the CNIL decided that the ISS mechanism did not apply and that the CNIL was therefore competent to make a decision. According to the CNIL this means that for non-EU companies having administrative headquarters in the EU only, no main establishment can be identified and no lead SA under the ISS mechanism can be established (Lead SA). To support its view, the CNIL refers to the guidelines for identifying a Lead SA as issued by the European Data Protection Board (EDPB Guidelines).

WHAT IS THE ISSUE?

The question is whether the CNIL (in reliance on the EDPB Guidelines) is right to require that, for the ISS mechanism to apply, the EU administrative headquarters has to determine the purposes and means of the relevant cross-border processing (and therefore also has to qualify as

---

1 Lokke Moerel is Professor of Global ICT Law at Tilburg University and Senior of Counsel at Morrison & Foerster in Berlin. Ms. Moerel thanks Karine e Silva for her assistance with research and footnotes.
2 CNIL (21, January 2019), Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l’encontre de la société Google LLC.
3 The one-stop-shop mechanism is codified in Art. 56 GDPR: ‘the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the [cooperation] procedure provided in Article 60.’
5 Article 29 Working Party (16, December 2016), Guidelines for identifying a controller or processor’s lead supervisory authority (as last revised and adopted on 5 April 2017) (WP 244), as endorsed by the EDPB in its first plenary meeting (Endorsement 1/2018) (EDPB Guidelines).
If that is correct, the 1SS mechanism will *de facto* not be available for non-EU headquartered companies (such as Google), as their EU administrative headquarters will rarely independently decide on the purposes and means of its cross-border processing activities in the EU. (These activities are often part of global service offerings in respect of which decisions are mostly made at the global level). This entails that these companies are exposed to a potential accumulation of fines for their cross-border processing activities in the EU, as each and every national SA would be able to fine the company up to the maximum allowed under GDPR. Though some may find that an acceptable outcome for non-EU headquartered companies, it is overlooked that the CNIL’s decision also severely impacts the availability of the 1SS for EU headquartered companies, also exposing these companies to a potential accumulation of fines.

As the CNIL’s decision will set a precedent for other enforcement actions going forward (e.g. the Information Commissioner’s Office (ICO) has announced a similar enforcement action against Google), it is of paramount importance to evaluate its merits.

This article argues against the interpretation given by the CNIL and proposes an understanding of the 1SS mechanism that is consistent with the rationale of the 1SS, the legislative history of the GDPR, and the regime for Binding Corporate Rules.

**Broader Context**

The main purposes for the European Commission (EC) to propose the GDPR, were the inconsistencies and fragmentation in the data protection laws of the EU Member States, and a goal of better governance through unification and simplification: ‘the 27 EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement’. The key changes proposed were a uniform set of rules across the EU and a 1SS for enforcement: ‘organisations will only have to deal with a single national data protection authority in the EU country where they have their main establishment.’ At the time of the adoption of the GDPR, the EC touted as the benefit for companies that the GDPR would bring a 1SS for businesses with cross-border processing operations in the EU: ‘companies will only have to deal with one single supervisory authority, not 28, making it simpler and cheaper for companies to do business in the EU.’ Though the 1SS does indeed bring benefits for companies, it obviously also benefits enforcement of rights of individuals by facilitating EU-wide enforcement by a single decision of one Lead SA. Given this increase in efficiency of enforcement, you would expect all SAs to

---

6 I focus on the 1SS for controllers. Article 56 also provides for a 1SS for processors, which presents its own issues and is outside the scope of this article.

7 The Telegraph (4 February, 2019). Britain’s data watchdog to investigate Google over privacy concerns.


12 See for the benefits of a 1SS, instead of several competent SAs, Balboni, Pelino, & Scudiero (2014), Rethinking the one-stop-shop mechanism: Legal certainty and legitimate expectation, Computer Law & Security Review, Vol. 30(4), p. 394: ‘In fact, involvement of several DPAs may generate confusion, conflicts in competence, escalation in
have been in favor of this concept, or so you would think. The reality was that many SAs opposed the 1SS mechanism, so much so that the 1SS actually proved to be the last hurdle for adopting the GDPR, requiring separate negotiation sessions and repeated drafts. The opposition was triggered by the realisation (belatedly) that not all Member States have an equal number of EU headquarters in their territories. The ones with more EU headquarters (mostly the northern Member States) would act more often as Lead SA, gain more control, and (most importantly) would also be able to collect the newly increased fines. This is all to the detriment of the SAs with fewer EU headquarters, which would lose their enforcement powers against the local subsidiaries in their territories. In order to ensure adoption of the GDPR, a compromise was ultimately struck which diminished the effectiveness of the 1SS. The Lead SA would no longer act independently, but would act as a ‘first among equals’, whereby other relevant SAs (e.g. with local establishments) could join in enforcement actions initiated by the Lead SA and (most importantly) receive their shares of the fines imposed. Note, however, that the core of the 1SS, whereby one Lead SA coordinates enforcement in respect of cross-border processing operations in the EU (to the detriment of the national enforcement powers of the SAs in their own territories) remained firmly in place.

**SUMMARY ASSESSMENT**

At first glance, the provisions and Recitals of the GDPR provide support for the decision of the CNIL. As is often the case, however, the provisions of the GDPR cannot be taken at face value but require a review of the legislative history of the GDPR and the underlying rationale of the relevant provisions, in order to determine the correct application. In this case, the outcome is surprising. The conclusion is that the 1SS also applies to non-EU controllers having establishments in the EU (which per definition then do not make decisions about purposes and means). Enforcement against such non-EU controllers is then possible in their place of central administration in the EU, whereby the justification for enforcement against such central administration (rather than the non-EU controller), is the fact that such central administration in the EU has the corporate power to ensure the implementation of compliance by the establishments in the EU, thereby greatly enhancing practical enforcement in the EU against non-EU controllers.

The requirement of the CNIL that the central administration in the EU must also make decisions

---

13 See also Balboni, Pelino, & Scudiero (2014), Rethinking the one-stop-shop mechanism: Legal certainty and legitimate expectation, Computer Law & Security Review, Vol. 30(4), p. 396: ‘We understand that, behind the resistances to embrace a full OSS system, there may be the fear that some DPAs will somehow take the ‘lion’s share’ of the whole proceedings involving major controllers and/or the fear that such a model implies a loss of independence or powers for the (other) DPAs. As to the first point, this is basically a political issue rather than a legal one, and as such it should be addressed openly and frankly.’

about purposes and means therefore undermines the ISS as provided by the GDPR. This decision may be a short-term benefit to the CNIL and its national enforcement powers against Google but will ultimately prove detrimental to effective EU-wide enforcement (including uniformity in application and legal certainty) in the longer term. The SAs cannot have it both ways. The ISS cannot be applied when it suits them. Either there is an ISS enforcement option against Google (whereby the Lead SA in one single decision ensures EU-wide enforcement) or we go back to the pre-GDPR days where each and every SA needs to act against Google to ensure enforcement in its own jurisdiction. The GDPR stands for the first option, as expressed in Recital 97 (Initial proposal):  

(97) Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.’

The CNIL’s decision also impacts the availability of the ISS for EU headquartered companies, but in a slightly different manner. As things are complicated enough as they are, I will first discuss the CNIL’s decision as applied to non-EU companies and then address its impact on EU headquartered companies separately.

Support for the Position of the CNIL

Looking at the literal text of the definition of main establishment in Article 4(16)(a) of the GDPR, it may well imply that the central administration in the EU is the place where decisions about the purposes and means of the processing of personal data are made. This could be implied by the use of term ‘unless’, which could be taken to mean that if decisions on purposes and means of processing will be made by another establishment instead of by the central administration, such other establishment will qualify as the main establishment. See the definition of ‘main establishment’ in Article 4(16) of the GDPR:

‘(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;’

The same applies to GDPR Recital 36, which could be read as providing for more detailed criteria for the ‘main establishment’ regardless of whether this is the place of central administration or the establishment making decisions on the purposes and means of processing (see part in bold):

‘(36) The main establishment of a controller in the Union should be the

---

place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment.’

This seems to be confirmed by the EDPB in its Guidelines (though other parts of the EDPB Guidelines contradict this conclusion, see more on this below):\(^\text{16}\)

‘The approach implied in the GDPR is that the central administration in the EU is the place where decisions about the purposes and means of the processing of personal data are taken and this place has the power to have such decisions implemented.

The essence of the lead authority principle in the GDPR is that the supervision of cross-border processing should be led by only one supervisory authority in the EU. In cases where decisions relating to different cross-border processing activities are taken within the EU central administration, there will be a single lead supervisory authority for the various data processing activities carried out by the multinational company. However, there may be cases where an establishment other than the place of central administration makes autonomous decisions concerning the purposes and means of a specific processing activity. This means that there can be situations where more than one lead authority can be identified, i.e. in cases where a multinational company decides to have separate decision making centres, in different countries, for different processing activities.’

Below I will first analyse the GDPR provisions that are relevant to the CNIL’s decision against the background of their underlying rationale and the context of other provisions of the GDPR. This will show that the interpretation advocated in this article prevails. I will then analyse the legislative history of the relevant provisions which will confirm that the history of the drafting of the GDPR supports this alternative interpretation.

**The rationale behind the concept of ‘main establishment’**

The essence of the lead supervisory authority principle in the GDPR is (as also stated by the EDPB above)\(^\text{17}\) that the supervision of cross-border processing activities should be led by only

\(^{16}\) EDPB Guidelines, p. 5.
one supervisory authority in the EU in order to enhance consistency in application, legal certainty and reduce the administrative burden for controllers and processors. A rationale was added later that the benefit of a main establishment is ‘having a single decision across the EU and a single interlocutor for business and for the individual.’\(^\text{18}\) Note that the latter means enhancing the efficiency of enforcement against business, i.e. by facilitating central enforcement by the SAs on behalf of individuals.

**Controller Does Not Have to Be Established in the EU**

The GDPR is set up in such a manner that its provisions apply regardless of whether the controller or processor itself is established in the EU. It is sufficient that the personal data is processed in the context of an EU establishment of a non-EU controller. This is not immediately obvious from the provision itself.\(^\text{19}\) See Art. 3(1) GDPR:

> ‘This regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.’

However, the legislative history of the provision, case law of the European Court of Justice (ECJ) (the Google Spain case)\(^\text{20}\) and the EDPB Guidelines on territorial scope\(^\text{21}\) confirm that for applicability of the GDPR it is not required that the controller itself is established within the EU:

> ‘i) Relationship between a data controller or processor outside the Union and a local establishment in the Union

The activities of a local establishment in a Member State and the data processing activities of a data controller or processor established outside the EU may be inextricably linked, and thereby may trigger the applicability of EU law, even if that local establishment is not actually taking any role in the data processing itself.’

In wording similar to that found in the scope provision of Article 3 of the GDPR, the definition of ‘main establishment’ does not say that the controller itself should be established in the EU.

---

\(^\text{17}\) EDPB Guidelines, p. 5.


\(^\text{19}\) See on this extensively in respect of the predecessor to article 3(1) GDPR in the EU Data Protection Directive (which was nearly identical); Moerel, Lokke (14, February 2014), Big Data Protection, How to Make the Draft EU Regulation on Data Protection Future Proof, Oratie Universiteit Tilburg.


\(^\text{21}\) European Data Protection Board (16 November, 2018), Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). Version for Public Consultation, p. 6. The main applicability rule of Article 3(1) GDPR has remained the same as under the EU Data Protection Directive and the European Parliament and Council did not propose any amendments to the initial proposal of the Commission. As a consequence, the legislative history of the GDPR does not explicitly discuss this provision. The guidance now given by the EDPB is fully aligned with earlier guidelines issued by the predecessor of the EDPB and the case law of the CJEU issued in respect thereof.

just that the controller must have establishments in more than one Member State. In a case of a non-EU controller having establishments in the EU, these establishments may therefore not qualify as controllers in their own right (they may even not have any role in the data processing itself).

The definition of main establishment, clearly also covers the situation where the controller itself is outside the EU:

‘as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and this establishment has the power to have such decisions implemented’

In establishing a ISS for non-EU controllers, the best port of call for ISS enforcement would be its EU headquarters, which has corporate control to direct compliance within its EU group of companies. Instead of the EU headquarters, the EU legislators, however, opted for the term ‘central administration’ in order to ensure that institutions where there is no official legal EU headquarters, another establishment could be identified as best placed (in terms of management functions and corporate controls) to qualify as the main establishment, therefore guaranteeing the ISS enforcement also against non-EU controllers.

Read from this perspective, it is clear why the ISS mechanism does not specify that the central administration in the EU must decide the purposes and means of processing. The provision may well cover non-EU controllers, whereby these decisions may be made by such non-EU controller.

This is also the logical interpretation of why ‘the place of central administration in the EU’ is included in the provision in the first place. If the EU regulators had intended that the central administration should make decisions on purposes and means (as the CNIL assumes), the provision could have simply read that the main establishment for a cross-border processing is ‘the establishment in the EU deciding on purposes and means of the relevant cross-border processing’ (or even shorter: ‘the EU establishment being the controller of the relevant processing’). The reference to ‘the place of central administration’ would have no function. The inclusion of the place of central administration must therefore mean something different than the reference to ‘establishment where the decisions on purposes and means of the relevant processing are taken’ (referring to who qualifies as the controller), as otherwise why include this element in the provision in the first place? This argument also works the other way: if the place of central administration would also be the place where decisions on purposes and means are taken, why include the alternative option? The alternative option would be irrelevant.

The construction is only consistent if the place of central administration is understood as the place where corporate control is exercised and compliance can be streamlined across establishments. In this interpretation, the alternative option has significant relevance as enforcement against the latter establishment is more efficient than against the EU center of administration, as it can both decide on purposes and means and also have these decisions implemented. Note also that the alternative option is different from mere controllership; the

23 A similar use of wording is also adopted in the definition of cross-border processing in Art. 4(23) GDPR.
24 See Recital 37 of the GDPR.
controller needs to be in the EU itself and further also have the power to implement decisions. The underlying rationale again is how to best enforce decisions throughout the EU (ensuring the power to direct compliance) rather than by first and foremost identifying the party having the legal responsibility to comply with the GDPR (i.e. the controller).

The above interpretation is confirmed by Recitals 36 and 37 of the GDPR, which provide a clarification for which entity of a group of undertakings qualifies as the main establishment. These Recitals make clear that where processing is carried out by a group of undertakings, the establishment of the undertaking in the EU with overall control over the EU establishments should be considered to be the main establishment for the group, which is based on the legal and decision structure of the relevant group of companies and therewith powers to have data protection compliance implemented, rather than that this establishment is itself making the decisions on purposes and means. See the last sentence of Recital 36:

‘Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.’

See also Recital 37:

‘A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.’

As indicated before, the EDPB Guidelines on identifying the Lead SA are at times contradictory. Though the EDPB expressly states that the main establishment should make decisions on purposes and means, other passages of the EDPB Guidelines are in contradiction and actually support the interpretation given in this article.

- As a first example, the EDPB Guidelines state that GDPR Recital 36 is useful in clarifying the main factors that shall be used to determine a controller’s main establishment if the criterion of the central administration does not apply, and subsequently lists the ‘objective’ factors as referred to in the second sentence of Recital 36 (see the part in italics in citation above):
  - Where are decisions about the purposes and means of the processing given final ‘sign off’?
  - Where are decisions about business activities that involve data processing made?
  - Where does the power to have decisions implemented effectively lie?
  - Where is the Director (or Directors) with overall management

---

responsibility for the cross border processing located?

○ Where is the controller or processor registered as a company, if in a single territory?

The EDPB apparently interprets the second sentence of GDPR Recital 36 to apply only when deciding on the alternative main establishment (where decisions about purposes and means are made and can be implemented), in the cases when there is no place of central administration in the EU (considering these factors thus not relevant for deciding whether there is a central administration in the first place). This contradicts the argument that Recital 36 would support the interpretation given by the CNIL.

Also in line with the aforegoing, the EDPB\textsuperscript{26} discusses \textbf{borderline situations} “where it is difficult to identify the main establishment or to determine where decisions about data processing are made. This might be the case where there is cross-border processing activity and the controller is established in several Member States, but \textbf{there is no central administration in the EU} and none of the EU establishments are making decisions about the processing (i.e. decisions are made exclusively outside the EU). And, even for those situations, the EDPB provides for a solution to ensure a 1SS. In those cases, according to the EDPB, the non-EU controller can actually \textbf{appoint} a main establishment in the EU, very much along the lines as provided for in the regime for Binding Corporate Rules (BCR), where a non-EU headquartered company can appoint an ‘EU headquarter with delegated data protection responsibilities’, against which any non-compliance of the group can be enforced (see more BCR requirements below). In the words of the EDPB:\textsuperscript{27}

\begin{quote}
‘In the case above, the company carrying out cross border processing may be keen to be regulated by a lead authority to benefit from the one-stop-shop principle. However, the GDPR does not provide a solution for situations like this. In these circumstances, the company \textbf{should designate the establishment that has the authority to implement decisions about the processing activity and to take liability for the processing, including having sufficient assets}, as its main establishment. If the company does not designate a main establishment in this way, it will not be possible to designate a lead authority. Supervisory authorities will always be able to investigate further where this is appropriate.’
\end{quote}

\textbf{LEGISLATIVE HISTORY}

The interpretation given in this article is supported by the legislative history of the relevant provisions. Notably, the EC in its initial proposal for the GDPR (\textit{Initial Proposal})\textsuperscript{28} provided for a more extensive 1SS mechanism,\textsuperscript{29} whereby the SA:

\begin{quote}
‘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.’
\end{quote}

\textsuperscript{26} EDPB Guidelines, p. 8.
\textsuperscript{27} EDPB Guidelines, p. 8.
\textsuperscript{28} European Commission (25 January 2012). COM(2012), 11 Final (\textit{Initial Proposal}).
Recital 97 provided the rationale, which has remained the same (see citation above). The 1SS mechanism was therefore initially intended to apply to all processing activities in the EU, and was thus not limited to cross-border processing activities only. The 1SS would also apply to local-for-local processing activities in the Member States.

The definition of ‘main establishment’ in the Initial Proposal, however, very much deviated from the final provision in the GDPR: initially, the main establishment of the controller was the place of its establishment in the EU where the main decisions as to purposes and means are made, and in contrast for processors, the place of its central administration. The interpretation now given by the CNIL was therefore fully in line with the definition in the Initial Proposal, but this provision changed drastically thereafter. Further note that already in this first draft the ‘place where decisions are taken’ (for controllers) was meant to have a different meaning from the expression ‘place of central administration’ (for processors).

See Art. 4 (13) of the Initial Proposal:

’main establishment’ means as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, “main establishment” means the place of its central administration in the Union;’

The comment of the European Data protection Supervisor (EDPS) in respect of the definition of ‘controllers’ under the Initial Proposal recommended further refining the criteria to identify a controller’s main establishment:30

‘refine the criteria to identify the main establishment of the relevant controller, taking into account the ‘dominant influence’ of one establishment over others in close connection to the power to implement personal data protection rules or rules relevant for data protection. Alternatively, the definition could focus on the main establishment of the group as a whole.’

In other words, not so much the decisions on purposes and means should be relevant according to the EDPS, but rather the power to get data protection rules implemented (i.e. ‘dominant influence’) should be relevant here.

This input was taken to heart by the European Parliament (EP), which in its first reading31 amended the definition for main establishment as follows:

‘main establishment’ means as regards the controller, the place of its establishment the place of establishment of the undertaking or group of undertakings in the Union, whether controller or processor, where the

30 European Data Protection Supervisor (7 March 2012), Opinion of the European Data Protection Supervisor on the data protection reform package, p. 69.
main decisions as to the purposes, conditions and means of the processing of personal data are taken. If no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, ‘main establishment’ means the place of its central administration in the Union. The following objective criteria may be considered among others: the location of the controller or processor’s headquarters; the location of the entity within a group of undertakings which is best placed in terms of management functions and administrative responsibilities to deal with and enforce the rules as set out in this Regulation; the location where effective and real management activities are exercised determining the data processing through stable arrangements.’

The reference to ‘main decisions as to purposes and means’ remained, but the subsequent criteria made it clear that for this criterion to be met, a number of objective criteria would be relevant. These objective criteria went well beyond whether the relevant company decided on the purposes and means and included the location of the controller’s headquarters, the location of its management functions and its administrative responsibilities to deal with and enforce the rules. After the EC’s consultations with the Council, the definition of main establishment was changed into its current form, making the place of central administration the main establishment also for controllers (aligning this with the connecting factor for processors), unless decisions on purposes and means are made by another establishment in the EU, and adding the element that such establishment has the power to have such decisions implemented.

The EC communication to the EP concerning the adoption of the GDPR by the Council explains that these changes are still in line with the original purposes:

‘One-stop-shop: a 'one-stop-shop' for businesses: companies will only have to deal with one single supervisory authority, not 28, making it simpler and cheaper for companies to do business in the EU.’

Moreover, the agreement reached on the ‘one-stop-shop’ mechanism is legally and institutionally sound, and brings significant added value for companies and data subjects. The mechanism will rely on the principle of the ‘best placed authority’ to take the decision and it will focus only on cases with an important cross-border dimension. The outcome in Council maintains the key simplification element of having a single decision across the EU and a single interlocutor for business and for the individual.’

The desired efficiency for businesses and individuals (and therefore also for SAs) applies equally to EU headquartered and non-EU headquartered companies. Indeed the relevant provisions of the GDPR have never been limited the 1SS mechanisms, nor was this option ever discussed as part of the legislative history. The CNIL by requiring that the place of central administration has to also decide on purposes and means, unduly limits the 1SS to non-EU headquartered companies.

only. This is ultimately detrimental to efficient enforcement throughout the EU.

**ALIGNMENT WITH BCR REGIME**

As a side note, I mention that the concept of the ‘place of central administration’ in the EU is in line with the supervision and enforcement regime developed by the predecessor of the EDPB (the WP29) when developing the concept of BCR as an alternative data transfer tool for intercompany data transfers (which is now fully codified in the GDPR). To ensure that the BCR can also be easily enforced in a case of non-EU headquartered companies, the BCR requirements\(^ {33}\) require that such non-EU company appoint an “EU headquarters with delegated data protection responsibilities” (EU Delegated HQ). This concept is based on the assumption that decisions on purposes and means may well be made by the non-EU controller, but still ensures that efficient enforcement in the EU is achieved by having an EU Delegated HQ where BCR violations can be enforced. Also under the BCR regime, a 1SS mechanism is ensured, whereby the SA of the EU Delegated HQ acts as Lead SA for the EU BCR authorisation procedure and is subsequently tasked with central supervision of the BCR. The WP29 BCR opinions specify the factors which are considered relevant for deciding which SA is best placed to act as Lead SA for the BCR authorisation procedure (to avoid forum shopping).\(^ {34}\) In case a company has its headquarters outside the EU, the most appropriate choice of an SA should be addressed, which has to be decided based on a number of factors, whereby it is explicitly stated that priority will be given to the first factor, being the location of the EU headquarters of the company. Corporate control to ensure implementation of compliance is apparently prevailing. It is also noteworthy that the third factor is covering the situation where there is no such official legal EU headquarters:\(^ {35}\)

> ‘3.3.3 the location of the company which is best placed (in terms of management function, administrative burden etc.) to deal with the application and to enforce the binding corporate rules in the group;’

Again, corporate governance and administrative functions take precedence over legal controllership responsibility for the processing itself.

**IMPACT ON EU HEADQUARTERED COMPANIES**

Though the CNIL’s decision seems of relevance to non-EU companies only, it also severely impacts the availability of the 1SS for EU headquartered companies. The fact is that the EU

\(^ {33}\) See Article 29 Working Party (29, November 2017), Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (WP 256) and Article 29 Working Party (29, November 2017), Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (WP 257), as last revised and adopted on 6 February 2018.

\(^ {34}\) See Article 29 Working Party (14, April 2005), Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules (WP 108) and Article 29 Working Party (11, April 2018), Working Document Setting Forth a Co-Operation Procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR (WP 263) (referring to the same criteria for deciding on the lead supervisory authority as listed in Article 29 Working Party paper WP 108 and as repeated in Article 29 Working Party paper WP 263). Note WP 256, 257, and 263 were all endorsed by the EDPB in its first plenary meeting (Endorsement 1/2018).

headquarters of an EU company does not in all cases decide on the purposes and means of a cross-border processing activity. These decisions may well be made by one of its local establishments (mostly being a subsidiary of the EU headquarters). In such cases the interpretation by the CNIL of ‘place of central administration’ will lead to a mutually exclusive situation where no Lead SA can be identified for these cross-border processing activities at all: the main option (place of central administration) would not apply since the EU headquarters does not make decisions on purposes and means, but neither would the alternative option (establishment making decisions), since the local establishment would not have the power to implement decisions. This interpretation is at odds with the rationale for the ISS mechanism, which is clearly intended to always lead to a main establishment regarding a cross-border processing activity. This can also be derived from the drafting of the definition of main establishment, where the options are not equal alternatives: the main option is intended to be the default solution, unless the alternative option applies. Again, the construction is only consistent if the place of central administration is understood as the place where corporate control is exercised and compliance can be streamlined across establishments.

**CONCLUSIONS**

This article opposes the interpretation of Art. 4(16)(a) given by the CNIL in its decision of 21 January 2019 against Google. The alternative interpretation presented in this article offers a holistic understanding of the legal text, the rationale behind the ISS mechanism, and the legislative history of the GDPR read in conjunction. Following the interpretation defended here, the Google EU administrative headquarters should have been recognised as the place of central administration of the controller in the EU. Recognizing the Irish entity as place of central administration for the undertakings in the EU would have triggered the application of Article 56 of the GDPR to establish the Irish SA as the lead authority in the case.

***

**BIBLIOGRAPHY**


Article 29 Working Party, (16, December 2016), Guidelines for identifying a controller or processor’s lead supervisory authority (as last revised and adopted on 5 April 2017) *(WP 244)*, as endorsed by the EDPB in its first plenary meeting (Endorsement 1/2018).

Article 29 Working Party, (29, November 2017), Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules *(WP 256)*.

Article 29 Working Party, (29, November 2017), Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules *(WP 257)*.

Article 29 Working Party, (11, April 2018), Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data *(WP 264)*.

Electronic copy available at: https://ssrn.com/abstract=3337478


European Commission (25, January 2012), Commission proposes a comprehensive reform of data protection rules to increase users’ control of their data and to cut costs for businesses, Press Release.

European Commission (25, January 2012), COM(2012) 11 final, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

European Commission. (11, April 2016), COM(2016) 214 final. Communication from the Commission to the European Parliament pursuant to Article 294(6) of the Treaty on the Functioning of the European Union concerning the position of the Council on the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and repealing Directive 95/46/EC.


European Data Protection Supervisor (7, March 2012), Opinion of the European Data Protection Supervisor on the data protection reform package.


Moerel, Lokke (14, February 2014), Big Data Protection, How to Make the Draft EU Regulation on Data Protection Future Proof, Oratie Universiteit Tilburg.


The Telegraph (4, February 2019), Britain’s data watchdog to investigate Google over privacy concerns.