How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner?

A Reaction to Christopher Hodges

Hielke Hijmans*

I. Introduction

In his excellent contribution, Hodges explores a few essential questions around enforcement of data protection law in general and the General Data Protection Regulation (GDPR) in particular. The questions posed by Hodges are highly relevant. They aim at effectively delivering data protection. This aim is also at the core of Regulating for Results, a paper of the Centre for Information Policy Leadership (CIPL) paper to which both of us contributed.

Successful data protection requires effective supervisory authorities (data protection authorities, DPAs), working in a legitimate manner. This is a relevant issue, if only because of the wide responsibilities given to the DPAs which go far beyond strict enforcement tasks. The long list of DPA tasks in Article 57 GDPR illustrates this. For instance, DPAs have advisory tasks and even the task of raising awareness of data protection amongst the general public. However, the assignment of all these tasks is not accompanied by indications how they interrelate, nor by guarantees of sufficient resources to fulfil them in an effective and legitimate manner.

The views of Hodges are based on two overarching convictions developed in other areas of law. In the first place, regulators (such as DPAs) must act strategically. This does not only mean that DPAs themselves should work strategically, but also based on shared and consistent approaches between DPAs ensuring that they all operate in a similar manner. In the second place, this strategy must be based on trust and cooperation between these regulators and the organisations they supervise, not on deterrence. These convictions determine his criticism on the GDPR and on DPA practices.

II. Strategic Approaches

Hodges argues that the GDPR is silent about enforcement and compliance policies. This is a fully correct statement. However, this silence is the logical consequence of the complete independence as laid down in Article 8 Charter and Article 16 Treaty on the Functioning of the European Union (TFEU) and underlined in the case law of the Court of Justice of the EU (CJEU). Complete independence is directly related to the difficult policy considerations a DPA is required to make. The Court stated that complete independence is needed in view of the DPAs’ task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data. Hence, the Court underlines that establishing a balance between the various interests at stake is the essence of DPA independence.

The question therefore should not be whether the GDPR should have included an enforcement strategy – it should not – but whether the GDPR contains sufficient tools or incentives for DPAs to develop such a strategy, if possible consistent with strategies of other DPAs. The answer to this question has different components.

---

* Hielke Hijmans, Independent Expert; Senior Policy Advisor, Centre for Information Policy Leadership (CIPL); Of Counsel, Considerati Amsterdam; Brussels Privacy Hub; Formerly at European Data Protection Supervisor, Brussels. For correspondence: <hielke.hijmans@gmail.com>.


2 This was also a central theme in my book on art 16 TFEU, Hielke Hijmans, The European Union as Guardian of Internet Privacy (Law, Governance and Technology Series 31, Springer 2016).

3 art 52 (4) GDPR leaves it up to the Member States to ensure the necessary resources, without specifying what necessary entails.


First, Article 57 enumerates 22 DPA tasks, but it
does not address the need for enforcement strategies.
Article 70 on the tasks of the European Data Protec-
tion Board (EDPB) does not address this either. As
said, this is logical in view of the DPA independence.
However, nothing would have prevented the legisla-
tor to provide a DPA (and/or the EDPB) with the task
of adopting an annual strategy, without entering the
domain of providing directions for this strategy.

Second, the legislator did provide the EDPB - indi-
rectly - with some more strategic tasks. Article
70(1)(k) GDPR is of particular importance in this con-
text since it provides that the EDPB shall issue guide-
lines for the DPAs concerning the application of their
powers as included in Article 58 and the setting of
administrative fines.\(^6\) Since Article 58 GDPR includes
enforcement related powers (in paragraphs 1 and 2)
as well as authorisation and advisory powers (in para-
graph 3), these guidelines could also cover strategies
prioritising between the use of these powers.

Third, the DPAs have to draw up an annual pub-
lic report on their activities (Article 59 GDPR). This
report, which should for instance be transmitted to
the national parliament, will necessarily include jus-
tifications for how DPAs performed and how public
money is spent. Thus, Article 59 includes another in-
centive for acting in a strategic manner.

In short, although the GDPR does not require DPAs
to develop strategic approaches, it contains some in-
centives for doing this nevertheless. The limited DPA
resources, mentioned above, may be a further in-
centive to act strategically.

III. Consistency

Consistency is an important objective of the GDPR,
as rightly underlined by Hodges. The GDPR distin-
guishes two situations: national processing and
cross-border processing as defined by Article 4 (23)
GDPR. As far as national processing is concerned, the
GDPR does not contain any specific tool or incentive
for consistent approaches. However, the national au-
thorities will base their practices on common inter-
pretations, in particular the case law of the CJEU and
the guidance by the EDPB. Obviously, the guidance
produced by the Article 29 Working Party before 25
May 2018 on key notions of the GDPR will play an
important role in this context.\(^7\) Although the guide-
lines and recommendations of the Article 29 Work-
ing Party and the EDPB do not produce binding ef-
fect, one may assume that ‘they are not without any
legal effect. The national courts are bound to take re-
commendations into consideration in order to decide
disputes brought before them [...].’\(^8\)

The scope of the GDPR instruments for coopera-
tion and consistency in Chapter VII of the GDPR is
restricted to cross-border processing, the second sit-
uation mentioned above. This chapter contains im-
portant incentives for consistent approaches. Yet, they
have two flaws:

First, these are instruments with a limited effect,
not necessarily ensuring consistent application of EU
data protection law. The main instrument for enforce-
ment cooperation is the one-stop-shop mechanism
(Article 60 GDPR) which concentrates the responsi-
bility for enforcement of data protection with one
national DPA, the ‘lead authority’. It only contains
some incentive for consistency because it strength-
ens the enforcement cooperation between DPAs. All
concerned DPAs are entitled to raise objections. An
objective of the mechanism is ‘an endeavor to reach
consensus’.\(^9\) However, practice will have to tell how
effective this incentive will be.

In any event, the one-stop-shop mechanism may
result in dealing with a case in the consistency mech-
anism before the EDPB. Despite its name, one can
question whether the latter mechanism is designed to
deliver consistency in enforcement.\(^10\) Article 64 (2)
GDPR allows any data protection issue to be handled
by the EDPB, resulting in an EDPB opinion. It does
however not contain any obligation to refer issues of
wider EU interest to the EDPB. Article 65 GDPR pro-
vides for dispute resolution resulting in a binding
EDPB decision. As the title of Article 65 explains, this

---

6 The latter task is already now taken up by the Article 29 Working
Party which set up a fining task force with as mandate the har-
monisation of calculating the administrative fines, ‘Article 29
Working Party – November 2017 Plenary Meeting’ (Press release,
=48748> accessed 5 March 2018.
newsroom/just/item-detail.cfm?item_id=50083> accessed 5
March 2018.
8 Joined cases C-317/08, C-318/08, C-319/08 and C-320/08 Alassi-
ni and Others [2010] ECLI:EU:C:2010:146, 40, with reference to
Case C-322/08 Grimaldi [1989] ECLI:EU:C:1989:646. This case
law is all the more relevant since the EDPB will be an EU body
[art 68 (1) GDPR].
9 art 60 (1) GDPR.
10 See in more detail, Hielke Hjimans, ‘The DPAs and their coopera-
tion: how far are we in making enforcement of data protection
provision is meant to solve disputes, not to develop consistent approaches. Even more so, the threshold for entering into dispute resolution is deliberately high. The article was drafted with the mindset that the dispute resolution should not be overburdened.\(^\text{11}\)

Second, these instruments primarily envisage consistent application of the law, not consistent strategies. The consistent application of the law which is a key objective of the DPAs in Article 51 (2) GDPR concerns primarily the consistency of the interpretation, for instance in order to avoid that certain processing operations will be subject to different requirements depending on which DPA is competent.

Seeking for a consistent strategy obviously goes further, as is also illustrated by Hodges’ contribution. A consistent strategy also deals with questions relating to the choices between performing different tasks. For example, does a DPA focus on consulting with data controllers of processors or on using enforcement tools?

\section*{IV. On Trust Instead of Deterrence}

Hodges explains in detail that trusted relations with regulated organisations should be the main pillar of the DPA work. Trusted relations should be based on a shared commitment on what is right and what is wrong and on evidence that each party can be trusted.

Hodges reasons that constructive engagement is the best way of actually affecting future behaviour.

This links to the CIPL paper which distinguishes four DPA roles: leader, authoriser, police officer and complaint-handler. It juxtaposes the leader and the police officer role,\(^\text{12}\) arguing that the role of leader should come first. In order for this leader role to be successful, constructive engagement with stakeholders and responsiveness are key attitudes for DPAs. I completely agree, but also consider that this is not the entire story.

However, successful leadership also requires this constructive engagement to be based on strength. I would call that a second pillar. DPAs should be in a position to lead or, as Hodges underlines, possess the ability to influence. They should be taken seriously as authoritative champions.\(^\text{13}\) This is also a reason why having sufficient DPA resources is a prerequisite for being an effective leader.\(^\text{14}\)

This second pillar also means, in my view, that hard enforcement through imposing strong sanctions\(^\text{15}\) should always be a part of the DPAs’ toolbox. There is common understanding that hard enforcement may, in any event, be needed for two reasons. First, not all organisations necessarily invest in ‘doing the right thing’. Also, the CIPL paper underlines the importance of administrative sanctions which should be ‘mainly targeted on non-compliant activity that is deliberate, wilful, seriously negligent, repeated or particularly serious’.\(^\text{16}\) Second, enforcement powers should be exercised from time to time. Otherwise, they lose meaning.\(^\text{17}\)

This has an important background in the GDPR context. In the public perception of the GDPR the availability of strong sanctions plays a key role. The wide attention for the GDPR is also the consequence of the high maximum administrative fines in the Regulation. Anyone working in this domain is familiar with the €20 million or the 4% of the annual worldwide turnover included in Article 83 (5) GDPR. These fines are an important element of the narrative, also within organisations, to invest in data protection. Additionally, it is an incentive for organisations to ensure that the internal data protection officer (DPO) role has the weight which Article 38 GDPR envisages, as explained by the Article 29 Working Party.\(^\text{18}\) The same applies, to a lesser extent, to the corrective powers of DPAs in Article 58 (2) GDPR. If these powers are not used, the incentive to invest in data protection might lose ground.

Finally, a presumed lack of effectiveness of DPAs\(^\text{19}\), also due to the lack of DPA powers, was a
major driver for the Commission to propose the GDPR.20 Again, strong DPAs – willing to show their teeth when needed – will be regarded as serious interlocutors by stakeholders in the private and public sector.

V. Accountability and Ethical Behaviour

Hodges underlines the importance of ethical values. This is in line with thinking about the principle of accountability of Articles 5(2) and 24 GDPR, extending the responsibility of the data controller beyond mere compliance with the specific obligations of the GDPR.21 He mentions fairness as the most important ethical value. Fairness is also at the core of Article 8 of the Charter of the Fundamental Rights of the Union. The risk based approach which is at the heart of data controllers’ accountability can be seen as an expression of fairness.

Accountability and ethical behaviour should lead data controllers, but are equally important for DPAs. Independence of DPAs also implies responsibilities. DPA accountability is illustrated by another famous phrase from the Commission/Germany ruling on DPA independence: ‘the absence of any parliamentary influence over those authorities is inconceivable’.22 This quote illustrates that DPA independence does not take away the accountability vis-à-vis democratically chosen bodies.23

Moreover, the broad descriptions of tasks of DPAs in Article 57 GDPR reflect the objective of their existence which goes beyond compliance with the rules of data protection and aims at affecting behaviour.24 To give an example, awareness raising – of the public and of controllers and processors – has become an explicit DPA task.25

Arguably, it is this wider assignment of affecting behaviour that may push DPAs towards the outcome promoted by Hodges: an effective ethical culture where all stakeholders ‘do the right thing’ and where they cooperate in an ongoing commitment based on trust.

I would like to make two remarks on this commitment. First, ensuring commitment may be easier said than done since it is not at all evident that there exists a common understanding on what represents ‘the right thing’ in situations where the benefits of data processing need to be balanced with the risks for the individual. For instance, scholars warn that automated decision-making may de-humanise individuals or social processes and deprives them from influence over decision-making processes that affect them.26 Others underline the benefits of automated decision-making for society in the fourth industrial revolution with machine learning and artificial intelligence.27 The controversy on the nature of Article 22 (1) GDPR on automated decision illustrates this perfectly. Should this be a direct prohibition for data controllers or is it a right that should be actively invoked by the data subject?28 The answer to this question relates directly to a specific understanding of what ‘the right thing’ means.

Second, possibly we do not need to pose the question whether a common understanding of the ‘right thing’ exist. Arguably, it is the intention that counts. As Kant wrote: ‘Nothing in the world – indeed nothing even beyond – can possibly be conceived which could be called good without qualification except a good will.29 The intention or good will should be a willingness to trust and cooperate with all those having a justified interest in questions relating to data use and data protection.

Hodges focuses in his contribution on a constructive engagement involving business and supervisory authorities. However, this ‘platform of the willing’ should possibly be much wider and also include civi-

---

20 Hijmans, The European Union as Guardian of Internet Privacy (n 2) 7.11.1.
22 C-518/07 Commission v Germany (n 5) 43.
24 Hodges calls this social behaviour in this context. More generally, he distinguishes between compliance and influencing behaviour.
25 arts 57 (1)(b) and 57 (1)(d) GDPR.
28 According to the Article 29 Working Party it is a direct prohibition; according to the Centre for Information Policy Leadership it is a right to be invoked. See ibid.
29 Immanuel Kant, Groundwork of the Metaphysics of Morals (The Liberal Arts Press 1939) 9, first sentence of ch 1.
il society and government in its role as data controller. Democratically chosen bodies should play their role. This is not only in line with the case law of the CJEU quoted above, but also the consequence of the fact that ethical choices around data processing in a rapidly developing digital society concern us all.

VI. The Specific Problem Relating to Complaint Handling by DPAs

The right of an individual to lodge a complaint is an important component of EU data protection law. Article 77 GDPR lays down this right as a remedy available to the data subject, next to the effective judicial remedies of Articles 78 and 79 GDPR. The CJEU also underlined the importance of this remedy where it ruled in Schrems30 that complaints of individuals should be examined with due diligence.

Although this does not mean that a DPA should investigate each and every complaint,31 complaint handling by DPAs is a recurring concern because it is demand led. A DPA cannot programme in advance the resources needed for complaint handling. Moreover, this task risks to absorb much of the DPA resources, making it impossible for DPAs to perform the variety of tasks in a strategic manner.

The requirement of due diligence in the Schrems ruling does, in my view, not necessarily mean that DPAs examine complaints themselves. The DPAs could develop a strategy which includes advising the complainants to consider alternatives, such as addressing a complaint to the controller or processor concerned who could be better placed to deal with a complaint.

From this perspective, it would be worthwhile to give further thought to Hodges’ suggestion for an industry-funded independent ombuds system. Such an ombuds system could not only be cost effective, but also be beneficial for data subjects (because it is quick and informal) and for controllers and processors (who would receive valuable feedback on their data protection related efforts). In addition, such an ombuds system would be equally useful for the public sector and for not-for-profit organisations.

VII. Conclusion

The contribution of Hodges is helpful for understanding the roles of supervisory authorities. His piece, based on models of general regulatory theory, could encourage the DPAs to work in a strategic and consistent manner. This reaction to Hodges supports this endeavour, by introducing some further thoughts which are specific for data protection. It provides considerations relating to strategic and consistent approaches in this area.

However, these specificities also demonstrate that Hodges’ argument should be applied in a nuanced manner in the area of data protection. This reaction explains that:

- trust should be at the core of DPA performance but strong sanctions – to be imposed in a proportionate manner in limited and exceptional cases – cannot be missed;
- ethical approaches are key and require involvement of actors beyond the DPAs and business, because of the huge societal implications of data use and processing;
- complaint handling is an essential component of DPA work; further thinking is needed on how to deal with complaints, for instance through the ombuds system proposed by Hodges.

---

31 This was previously the case in Spain, Artemi Rallo Lombarte, ‘The Spanish Experience of Enforcing Privacy Norms: Two Decades of Evolution from Sticks to Carrots’ in David Wright and Paul De Hert (Eds), Enforcing Privacy: Regulatory, Legal and Technological Approaches, (Law, Governance and Technology Series 25, Springer 2016) 126.