Unwarranted requirement of an accredited external monitoring body hampers establishing Codes of Conduct

Why this blog

Article 40.1 of the GDPR states that Codes of Conduct should be encouraged. The first 'evaluation' of the GDPR by the European Commission[1] and the recent evaluation of the Dutch GDPR implementing Act[2] underscore the importance of a Code of Conduct not only to strengthen the position data subjects but also to give all stakeholders more clarity about the specific meaning of the terms of the GDPR and national implementing Acts for the sector covered by the Code of Conduct. However, four years after the GDPR became fully applicable, there are hardly any such Codes of Conduct. Not on the European level and not on the national level.[3] The promise of Codes of Conduct remains unfulfilled. In this blog I argue that the main reason behind this is that according to the EDPB Guidelines on Codes of Conduct and Monitoring Bodies[4] an accredited external and independent monitoring body (hereinafter: EIMB) of the Code of Conduct must be appointed *and* that this requirement does not follow from the GDPR.

The requirement of an EIMB is a real hindrance for Codes of Conduct

Mentioned Guidelines state that as per article 40.4 GDPR a Code of Conduct of conduct shall contain mechanisms which enable the body referred to in Article 41.1 to carry out its mandatory monitoring of compliance with – in short – the Code of Conduct. Sections 2 and 4 of article 41 contains provisions about such EIMB's. National authorities have published criteria for the accreditation which are first subject to consistence mechanism of article 63 GDPR (41.3). Establishing a sector specific EIMB then proves a costly affair. In a later stage the controllers of processors subject to the monitoring will have to pay for these costs (and in the end we will all pay for this). Just as with accreditation schemes where the auditors should also be independent and competent, the audited party pays for auditors looking through the files and doing the interviews. And how could an EIMB established in field which is very diverse, does not have one trade organisation or something similar, and is also short of funds such as health research. One might get all the ducks in a row for a Code of

[1] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition EN two years of application of the General Data Protection Regulation,Bussels, 24.6.2020 COM (2020) 264 final.

[2] Pro Facto, Hooghiemstra & Partners, *Bescherming gegeven? Evaluatie UAVG, meldplicht datalekken en de boetebevoegdheid*, Groningen/Den Haag 22 juni 2022', at section 6.2.1 . Publicly issued on September 6 2022 as: Bijlage bij Kamerstukken 32761, nr. 246. Also available via https://pro-facto.nl/meer-actueel/924-evaluatie-uavg-aangeboden-aan-de-tweede-kamer

[3] Ibid

[4] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, Version 2.0, 4 June 2019

Conduct, which is already a very tedious process as I know from experience, but that EIMB with all the connected costs is a bridge too far.
Hence, as was also the experience with the Dutch draft Code of Conduct on health research, and not neglecting the difficulties of the consensus process when drafting a Code of Conduct, the requirement of an EIMB is the real hindrance to submit the Code of Conduct to a Supervisory Authority. And many sectors, foreseeing this, will simply have refrained from starting the time-consuming drafting process.

The EDPB fell short on sound legal reasoning that the EIMB is a requirement for a Code of Conduct
The next and more important issue is whether the GDPR really requires that a Code of Conduct is linked to an EIMB.
As seen, the EDPB points to the 'shall' in 40.4. However, article 41.1 states that the monitoring of a Code of Conduct *may* (my emphasis) be carried out by a body which has the qualifications mentioned in that article. The EDPB Guidelines do not mention the 'may' in 41.1 and do not discuss the apparent contradiction with the 'shall' of 40.4. One can only guess why the EDPB did not do so. They can impossibly have missed it. Whatever the reason, already because of this the Guidelines fall short on sound legal reasoning.

What conclusion can be reached if one applies sound doctrinal legal reasoning
But it gives us the change apply that reasoning on which the EDPB fell short. Lawyers do not like apparent contradictions in the law, certainly not in one and the same Act[5] and have established means to resolve them though that is not simply omitting a term which you apparently don't like.
Before I mention the overarching criterion, let us first look at the intention of legislator/history of the Act as one of those lawyers' tools. In this case that intention would be shown in the Recitals. The Recitals mentioning a Code of Conduct do not mention that a Code of Conduct is inextricably linked, to quote a term of the EDPB in another context, to an EIMB. Actually, they do not mention an EIMB at all. Recital 98 mentions the that a Code of Conduct should take into account the specific needs of SME's and micro enterprises. It is difficult to see how those would be helped with an expensive EIMB. In article 27 of Directive 95/46/EC Codes of Conduct were also encouraged. Articles 40 and 41 of the GDPR expand on that article of the Directive but there is no indication that the legislator would completely change the system of Codes of Conduct in that sense that a Code of Conduct can only be approved together with an EIMB. If so, one would assume that this would at least be reflected in the Recitals as the GDPR does on many other issues. The conclusion is that this way of interpretating the law points at that the 'shall' in 40.4 should yield to the 'may' in 41.1

Another tool would be that interpretation which gives the most protection. In this case that would be first of all the data subjects. I conclude to a draw here. It might be argued that a

[5] The discussion here is limited to that issue. Sometimes subsequent Acts have conflicting provisions and are both still applicable. Or a new Act may revoke an older one with provisions conflicting with the older one without a proper 'grandfather clause'. But the solutions for those cases are only indirectly relevant here.

Code of Conduct with an EIMB gives more protection than a Code of Conduct without an EIMB. Yet, if because of the necessity of an EIMB, there will no Code of Conduct, it can also be argued that the protection becomes less as data subjects will have less clear guidance about their rights on the issues covered by the Code of Conduct and will not have been consulted about those issues[6]. Data subjects are not the only stakeholders. Those are also data controllers, data processors and their employees who would be more helped with a Code of Conduct to navigate them through the GDPR in a compliant way without an EIMB than with no Code of Conduct at all.

In absence of convincing support from the historical or the most rights protection interpretation method, the overarching criterion as I would state it is as follows: *that interpretation which in context of all the other relevant circumstances, deviates the least from the literal text of each of the conflicting clauses and makes most sense, meaning making the Act as a comprehensible whole again, of both clauses together.*[7]
The context is then as explained the intention/ historical and rights protection interpretation but also other relevant clauses. It should be mentioned that the link with the presumed obligation of appointing an EIMB is only made in 40.4. For the context is also relevant article 41.6 which excludes public authorities and bodies from the application of article 41. Hence the EIMB requirements do not apply to those. Yet, they might be involved in the same data processing operations as other non-public entities such as foundations in the case of health research. And to be transparent to the public they might want to be a 'code member' together will all the other entities which perform similar data processing. These public bodies might rely on certain – usually – national research exemptions, which should then be reflected in the Code of Conduct but for all the rest the GDPR remains applicable as tailored/explained in that Code of Conduct. But how could that be done if all the other members should be subject to an EIMB and the public bodies not? Easily, if the EIMB would not be a requirement.
Coming back to the criterion. According to that criterion the 'may' in 41.1 cannot be changed or interpretated in such a way that it becomes 'shall' without completely changing the text and neglecting the earlier discussed most likely intention of the legislator. Article 40.4, on the other hand, easily can. It should be read as (in italics my new text) "*If the Code of Conduct has appointed a monitoring body referred to in Article 41.1, then* the Code of Conduct shall contain mechanisms… etc. A sloppiness in the drafting of the GDPR would be redressed without any harm to the overall GDPR clauses and purpose.

What next
Obviously, this new light on the requirements for a Code of Conduct and on the EDPB Guidelines undermines the industry around EIMB's. It is confrontational for the EDPB and for those who follow the Guidelines as if those were Moses coming back from the mountain with the two tables and hence abstained from drafting a Code of Conduct or are struggling with the EIMB requirement or have made great expenses to establish one. It might also

[6] See Recital 99 which requires that data subjects should be consulted about the draft Code of Conduct.
[7] For those with more knowledge of jurisprudence than I have, this phrase seems to be derived from Dworkin but then from which of his writings. Or from somewhere else, such as Nieuwenhuis, Drie typen van rechtsvinding' which I read even longer ago. I didn't look it up, after all this is a blog. And if it is self-invented, even better.

confrontational to those businesses, such as accountancy firms, which see a new revenue opportunity in becoming an EIMB.

I wonder what the EDPB will do after reading this. Though I hope to be wrong, probably nothing. The solution should come from challenging the requirement of an EIMB before first at a national court as Guidelines as such cannot be challenged before a court. Other lawyers, feel free to be inspired by this blog in such a case. Regretfully, I didn't get that far. Would have loved so with our Dutch Code of Conduct on health research but our funds and stamina had run out. Others, who might like to use this blog, please refer to it. Our blogpost system does not allow for comments. SME you know. But my integrity will assure that relevant comments, also -though unlikely - from the EDPB, will be posted, though my stubbornness cannot exclude that a comment will be followed by a rebuke from me.

Evert-Ben van Veen
September 10 2022