Article 29 Working Party - Guidance document 16/EN wp243

Submission/commentary from private individual - 31 January 2017

Summary

1) Having considered the Article 29 Working Party's("WP29") GDPR-related guidance documents issued in December 2016, the author is happy to endorse much of it. A number of concerns remain. The most urgent of these relate to 16/EN wp243. The following issues are discussed in respect of DPO:
   a) professionalism
   b) expertise in data protection law
   c) independence and conflicts of interest
   d) contracts (it is submitted, if the guidance is followed, these might critically undermine all of the above)
   e) abilities
   f) core activities

Introduction, Modalities, and Declaration of Interests

2) My name is Stuart Ritchie[1]. In England and Wales I am a practising solicitor and non-practising barrister. I am a court advocate in inter alia private international law and data protection law. I have links with legislators, but these are pro bono and currently these do not include MEPs (which also were pro bono). Since July 2015 (i.e. pre-final draft GDPR) I have been teaching training courses (via PreterLex and Firebrand in which I hold no shares) in GDPR law and implementation at business and IT level. These are now commercial and supported by a certification examination on GDPR law based on a bank of 400+ questions set by myself. Having developed commercial software since the 1980s, I now have developed a technology-neutral methodology to support GDPR implementation by controllers, and (non-workflow) software consistent with that methodology to provide quantified financial risk assessment by way of automated data protection impact assessments (for the GDPR and other laws encoded into metadata) from privacy dataflow metadata. I am co-founder of a joint venture called GDPR 360 which offers this software as a service. As part of a "subscription" we can offer "DPO as a service".

3) I say these things in order to make it clear I fully accept that in this submission I am conflicted in many ways.

4) Since late 2014 (i.e. well before the GDPR final draft) I have been considering how to implement the GDPR and in particular the role of the DPO. In order to prepare our courses and services I have considered appropriate DPO recruitment issues, contractual provisions, and SLAs, for DPOs engaged by either contracts of service or contracts for services (the English law meaning of this sentence is discussed later). My conclusions are reflected in my teaching.

5) In this document I try to mitigate my conflicts by addressing myself as closely to the law as possible. I do in effect discuss what I teach, and why, because my interpretation of the law is critical to that teaching.

6) I try to avoid discussing my own products. I do note that the existence of certain technologies (by way of "state of the art" etc) might impact legal interpretation and, perhaps more importantly, absence of consideration of certain types of technology might negatively affect both interpretation and harmonization.

7) Likewise I do not discuss the DPO services we offer, but I note they are aligned to the points I make here.

Scope

[1] The author's formal qualifications are BA Hons BSc LLM (e-commerce law) GDL PDPLS. His Linkedin profile may be found at https://www.linkedin.com/in/sritchieprivacylawprivacyit/. He may be contacted at stuart.ritchie@gdpr360.com.

8) In this submission I make a number of observations and/or discuss a number of issues. The first three topics are perceived to be the most crucial:
   a) professional qualities
   b) expertise
   c) contractual issues, independence, and conflicts of interest generally and specifically
   d) core activities
   e) abilities to perform the statutory tasks

Professional qualities

9) I begin by noting that, in effect, the GDPR creates a new statutory office that bypasses much contract law and employment law, and is far more rigorous than company law. It is submitted that professionalism in such a new office is to be encouraged and articulated a little, rather than discouraged or ignored.

10) I therefore was disappointed to see the rather sketchy attention paid to "professional qualities" in the guidance. I was even more disappointed to see it characterised primarily in terms of expertise (addressed *post*). It is respectfully submitted the guidance quoted above is an unsustainable interpretation of the GDPR, in respect of the plain meaning of the Article 37(5) words (at least in English), and of purposive interpretation, and of the Recitals, and of harmonization alike.

11) I accept the guidance does at least mention "high professional ethics". However, and bafflingly, this is mentioned only under "Ability to fulfil its tasks" rather than under "Professional Qualities".

12) The complete guidance for professional qualities (p11) states "*Although Article 37(5) does not specify the professional qualities that should be considered when designating the DPO, it is a relevant element that DPOs should have expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR. It is also helpful if the supervisory authorities promote adequate and regular training for DPOs. / Knowledge of the business sector and of the organisation of the controller is useful. The DPO should also have sufficient understanding of the processing operations carried out, as well as the information systems, and data security and data protection needs of the controller. / In the case of a public authority or body, the DPO should also have a sound knowledge of the administrative rules and procedures of the organisation"*

13) Let us go back to first principles and interpret the GDPR text. As the guidance previously acknowledges (ibid) "Article 37(5) provides that the DPO '*shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39*'".

14) It is submitted "professional qualities" is to be interpreted as "the qualities to be ascribed to a professional".

15) What, then, is a "professional"? It is submitted that, in English law at least, it essentially means a member of a body all of whom both subscribe to a written code of conduct and inherently are subject to a disciplinary process that could deprive him or her temporarily or permanently of their livelihood as sanction for any breach of the collective code of conduct. A more succint, if redundant, phrase is "regulated professional".

16) Further or alternatively, what guidance do we receive from elsewhere in the GDPR? It turns out there are many discussions of "professional" in the Recitals. Without enumerating them, it seems the typical meaning ascribed to "professional" is that which in England would be described as a "regulated professional", especially doctors/health-care workers and lawyers: often, especially in the context of the definition of "large scale", sole practitioner professionals in the English sense.

17) Next we consider the meaning of first "and" of the sentence, appearing before ", in particular". It is submitted that the "and" is conjunctive, as is the second "and". the following list is, on the plain meaning of the words, a requirement **additional** to professional qualities.

18) Further or alternatively, the subsequent "in particular", just as with other lists within the GDPR prefixed with "in particular", indicates an open-ended list. The list is not closed. It respectfully is submitted that professional qualities ought not be excluded from any definition of professional qualities (GDPR or otherwise), and likewise that a narrow list of unrelated characteristics ought not be substituted for professional qualities.

19) Having characterised "professional", how might we identify persons holding professional qualities or, if you like, the "qualities of a professional"? In my submission the initial point of departure must be a canonical list, **for example** as follows:
    a) a person who is or recently has been a member of a professional body and has not been struck off that profession's roll of members by way of disciplinary action; or
    b) a person who satisfies a professional body or body defined in statute for that purpose, by independent accredited examination, that he or she can and will adhere to an code of conduct of professional standard breach of which could lead to deprivation of livelihood.

20) I have no particular commitment to the exact form of words, nor have I experience in drafting non-corporate constitutions. The point is to set out a practical way of approaching the issue from the correct starting-point, in a way that would not prevent the WP29 / EDPB from exploiting other Articles to create such a DPO profession, or a simulation of it by way of professional ethics examinations or such other device as may be appropriate.

21) It is submitted that enforcement of DPO professional qualities lies at the heart of the success of the GDPR, to the extent that without it we might as well revert to the "data protection official" of 95/46/EC which was dependent on Member State whim.

22) Finally on this topic, I note, from a position of ignorance, that the legal traditions of different Member States might diverge in interpretation of "professional qualities", and thus there could be a threat to harmonization.

23) Please note I briefly must revisit this issue as critical to my discussions of independence and contracts *post*.

24) For the reasons set out above I respectfully invite WP29 to consider clarifying and, as it may deem appropriate, changing or expanding some of its guidance on professional qualities before such guidance becomes final.

Expertise

25) The (English) test is "expert knowledge of data protection law and practices". A number of issues appear to arise out of this. I approach this in two ways:
    a) Expertise in theory and in Court
    b) Expertise in practice from May 2018

Expertise in theory and in Court

26) The following observations are made from practical experience of Court advocacy in respect of expert witnesses in foreign law, coupled with some foreseeable unintended consequences of the GDPR.

27) I restrict my observations to my practising jurisdiction, England and Wales. That said, I emphasize I do not suggest that expertise tests in the other UK jurisdictions, or those of other Member States, are of lower standard. On the contrary, I assume the standard is as high, and therefore the consequences will be similar.

28) In England, (for reference only) the civil litigation rules for expert witnesses are set out in Part 35 of the Civil Procedure Rules[2] and especially in the accompanying Practice Direction[3]. I do not formally summarise these, merely pick out practical points.

29) If after presentation of credentials, and hostile cross-examination, and any further questions from the Court on qualifications, curriculum vitae, experience, conflicts, etc, the Court is inclined to treat the witness as an expert, then that is final and the Court may take the expert witness testimony into account in its deliberations.

30) Conversely, the Court may, for any reason or no reason, decline to accept the putative expert's testimony.

31) There is no particular standard to be met: it is a practical test based on quality of available independent practitioners. The higher the perceived "quality" of the expert, the more likely the testimony will be credible.

32) There are no "special" rules for expert witnesses in foreign law. In practice I have seen only retired or part-time judges in the other jurisdiction, or very experienced advocates in that jurisdiction, or academic lawyers holding a doctorate (or for a specialist field LLM) in that jurisdiction.

33) It is submitted that, **in the long run,** the minimum qualification required, for a DPO to be acceptable as an expert witness, is likely to converge on the alternatives of either
    a) a LLM graduate in relevant area(s) of Union and/or Member State data protection law; or
    b) a Court advocate experienced in data protection advocacy in relevant jurisdictions

34) It is submitted that no courses currently available (including my own) can meet such a standard, other than university LLMs in data protection law.

35) Against any objection that a LLM is an impossibly high standard, I note that (at least in England) a law qualification is not a prerequisite for a LLM.

36) Unfortunately there are two further problems, both of which exacerbate the expertise issue.

37) If a data protection law expert in the GDPR and/or English law is called in an English Court, both advocates and judges will be perfectly capable of construing the law for themselves. Their acceptance of the expert inevitably will stray towards thoughts such as "do I think this lawyer is even competent, measured against myself"?

38) The second problem may be critical. Expert witnesses are called in order to give their expert opinion. The Court's evaluation of their expertise is, in effect, the standard by which their testimony can be taken into account.

39) However, against the backdrop of the GDPR, the Court's evaluation of a DPO's expertise becomes, ipso facto, determinative of the issue, at least for plaintiffs. If the Court considers that a DPO is not an expert in data protection law, that in and of itself seems almost conclusive of a GDPR breach by way of an alternative route.

40) While this scenario "moves the goal-posts" to the extent that the DPO arguably could not be called as an expert witness, there is nothing to stop a plaintiff calling the DPO anyway as a hostile lay witness.

41) For avoidance of doubt, the Court-specific issues raised are not a problem and I merely draw them to WP29's attention. That said, it is submitted that we ought to promote increasing DPO expertise as enthusiastically as possible, to avoid the office of DPO rapidly falling into disrepute via Court actions.

---

[2] https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part35
[3] https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part35/pd_part35

Expertise in practice from May 2018

42) Opinions vary dramatically as to the number of DPOs who must be appointed before, generally well before, May 2018. Anecdotally, however, all estimates I have seen put the total in multiples of tens of thousands.

43) Even were expertise in data protection law sufficient for a DPO (it is not), there clearly are insufficient academic training establishments to provide enough DPOs of the standard I have suggested will and ought to be required (LLM).

44) For this reason, all manner of dubious establishments (including of course my own) have sprung up purporting to train people in GDPR compliance, and in becoming DPOs.

45) Pragmatically, this is necessary as a transition measure. Though a little knowledge is a dangerous thing, in this context a little expertise may be better than none. However, it is submitted the courses lasting days, or even weeks, are wholly insufficient in the long run.

46) It is submitted a pragmatic transition measure ought not be permitted to become a de facto standard. I therefore urge WP29 to consider continuously increasing the "required" standard for DPOs up to (eventually) LLM standard, which will encourage academic institutions and controllers alike.

47) For avoidance of doubt, I do not sanction supervisory authority endorsement of such courses. There are many dangers there, not least in respect of direct litigation against the supervisory authorities themselves, even under the GDPR itself. I will take this matter up separately with material supervisors.

48) For the reasons set out above I respectfully invite WP29 to consider clarifying and, as it may deem appropriate, changing or expanding some of its guidance on expertise, before such guidance becomes final.

Contractual issues, independence, and conflicts of interest generally and specifically

49) For avoidance of doubt I see nothing wrong with WP29's guidance on conflicts of interest or independence, per se. Unfortunately, it is submitted that the guidance on so-called "service contracts" might be construed as undermining DPO independence, expertise and professionalism. I therefore treat these matters together.

50) First, I address a minor, and probably linguistic/translation error.
    a) In English law the phrase "service contract" is a nullity. There are only two kinds of contract using the word "service":
        i) a "contract of service", meaning a "master-servant", or "employer-employee" contract; and
        ii) a "contract for services", meaning a non-employment contract between any legal person and an "independent contractor" supplying services.
    b) "Services contract" is synonymous with "contract for services". "Service contract" is simply a nullity.
    c) This distinction may seem trivial, but it is submitted this confusion may cause endless mischief in English courts unless addressed.

51) Turning to the guidance on "DPO on the basis of a service contract" (p12), we see, in total:

    The function of the DPO can also be exercised on the basis of a service contract concluded with an individual or an organisation outside the controller's/processor's organisation. In this latter case, it is essential that ***each member of the organisation exercising the functions of a DPO*** *fulfils all relevant requirements of Section 4 of the GDPR (e.g.,* ***it is essential that no one has a conflict of interests****). It is equally important that each such member be protected by the provisions of the GDPR (e.g. no unfair termination of service contract*

for activities as DPO but also no unfair dismissal of any individual member of the organisation carrying out the DPO tasks). At the same time, individual skills and strengths can be combined so that several individuals, working in a team, may more efficiently serve their clients.
*For the sake of legal clarity and good organisation it is **recommended** to have a clear allocation of tasks within the DPO team and to assign a single individual as a lead contact and person 'in charge' for each client. It would generally also be **useful** to specify these points in the service contract.*[my emphasis]

52) There are a number of statements here that, it is submitted, deviate from both the letter and the spirit of the GDPR in a fashion that undermines professionalism, expertise, and independence alike.

53) My starting point is my previous submissions as to professionalism.

54) The second paragraph talks about "recommended" within the DPO organisation to have a lead contact and person in charge. In the context of professionalism, it is submitted that it ought to be mandatory for a professional to take responsibility: without a professional in charge, there can be no professionalism and the GDPR is breached.

55) Next, the final sentence says it would be "useful" to specify "these points" in the contract. It is submitted, again, that it ought to be mandatory. Without specifying a professional in the contract, it is submitted that the contractually appointed DPO will not be a professional and, necessarily, the GDPR is breached.

56) If that is right, then it follows *prima facie* there could be three possible scenarios for a lawful DPO appointment:
    a) a services contract with a named natural person professional satisfying the other criteria;
    b) a 3-way services contract with a named natural person professional satisfying the other criteria, using a non-natural legal person for administration and invoicing vehicle (sometimes arranging contracts for a number of DPO engagements with a number of different clients); or
    c) a contract with a professional firm (of lawyers, or accountants, or engineers, or doctors, or whatever), any of whom might or might not satisfy any DPO criteria, individually or collectively.

57) The first of these is, apparently, not discussed by WP29. This seems strange because it is the natural default. However, it is unexceptional so I let it rest.
58) The second of these is, apparently, not discussed by WP29. This seems strange because it is, I understand from conversations with DPOs, a common arrangement in Germany which I understand applies at least similar, if not model, DPO rules to that of the GDPR. I may be wrong on that but in any event I should say that where, for whatever reason, the first option is not preferred, this is the model I endorse, teach, and apply.

59) The final alternative, by implication, seems to be discussed by WP29, and by implication endorsed as not only acceptable but also, by implication, the preferred model. I set out below a number of issues with this model.

60) Unfortunately there is no suggestion that the firm should be professional. This, it is submitted, might lead automatically to GDPR breach.

61) Further or alternatively, the firm might be a professional firm, but there is no suggestion in the guidance that anyone, separately or collectively, be a professional. Likewise, this might lead automatically to GDPR breach.

62) Further or alternatively, there might be a professional in charge, and this further might be specified in the contract. However, without any engagement of the nominated professional in the contract by way of signature as a party, it is submitted that accountability issues might be raised to the same effect as before.

63) I further note from experience the commoditization of English so-called law firms, in areas such as motor insurance claims, such that the lawyer supposedly responsible for litigation can be six, sometimes seven levels up in the management and has no professional awareness at all, defeating the entire purpose of professional engagement. In other words, great care must be taken to avoid DPO engagements being "gamed" to defeat the spirit, and in my view letter, of the GDPR.

64) It might be suggested that no amount of gaming can defeat controller liability. That is so. But if WP29 produces guidance that facilitates such gaming, this might lead to "legitimate expectations" submissions from controllers and perhaps Member State-specific devices (such as, in England, estoppel). It is submitted we ought not set GDPR up to fail.

65) Further or alternatively, we must consider independence and conflicts of interest, not only in respect of professionalism generally, but also specifically in respect of the GDPR and emerging DPO case law.

66) Certain firms, indeed industries, have a poor track record with independence. Some, for example, might audit a firm at the same time they offer accounting services to it, despite rules on conflicts of interest. Some of these same firms and industries are offering DPO services. The guidance as written seems tailor-made for such firms.

67) Further or alternatively, there currently is nothing in the guidance to prevent DPO services firms from supplying services to competitors. This naturally raises conflicts of interest issues.

68) It might be suggested by such firms that they have existing internal processes in place to defeat such conflicts, often unedifyingly described by the firms as "Chinese walls". That is all very well. There are two difficulties here. The first is that they may not work. However there is a far more serious problem. These rules, as with company directors, are somewhat close to a low "standard" of independence: that of actual conflict. In my submission The way the jurisprudence is (rightly) moving is in the direction of the Bayern supervisory authority's 2016 fine of a controller for appointing an IT manager as DPO. The significance of this is that no actual conflict of interest seems to have been needed. A potential conflict was sufficient. it would seem to follow that internal processes necessarily must be insufficient to avoid perception of potential conflict.

69) Finally, the guidance implies that a DPO ought to be a team member. If that is right, then I would strongly dissent, whether the DPO is an employee or independent contractor. Teams imply conflicts and, almost as bad, management which itself creates conflicts, regardless of who is the manager and who are the managed. The solution, whether the DPO is internal or external, whether the "team" is internal or external, is sharply to separate them. This is very simple. The DPO is the DPO. Everyone else is in a separate body called, for example, the "DPO Liaison Team" which, of course, cannot be managed by the DPO.

70) For the reasons set out above I respectfully invite WP29 to consider fundamental changes to its guidance on services contracts, before such guidance becomes final.

<u>Core Activities</u>

71) I found WP29's guidance here invaluable: it widened the concept to the point that it will be consistent in practice with the objectives of the GDPR. I hope that guidance does not change.

<u>Abilities to perform the statutory tasks</u>

72) I do not take a point here. I simply list some of the "skills" I, from perusal of the GDPR and consideration against personal experience, have identified as useful for a DPO (depending on context), in the hope that WP29 finds it a convenient list. I regard the first six as the most critical, but otherwise ordering is arbitrary. I set them out as a "shopping list" rather than mandatory.

a) privacy impact assessments
b) compliance reviews
c) risk assessment and management
d) Dealing with supervisory authorities
e) Determination of whether issues should be placed before supervisory authorities
f) mediation
g) privacy by design
h) privacy by default
i) Information Architecture and dataflow mapping
j) Information security
k) Communications security
l) encryption at rest
m) Penetration testing
n) data breach
o) Training
p) audit
q) exchange formats
r) data analysis
s) Data modelling
t) data feeds / data migration
u) predictive analytics / business intelligence
v) "data science"
w) profiling
x) ability to read source code (deprecated in GDPR final)
y) ability to read system logs (deprecated in GDPR final)

End note

73) I am grateful to WP29 for hearing to what I have to say. I regret that time prevents me from setting out some suggestions on for example structure and modalities of Service Level Agreements, and non-DPO matters such as data portability (and how technically to handle legal issues such as mixed data).

Drafted this day 31 January 2017 by Stuart Ritchie