

D2.2 Report on best practices

Mahieu, René Louis Pierre; Borocz, Istvan Mate; De Hert, Paul

Publication date:
2021

License:
CC BY

[Link to publication](#)

Citation for published version (APA):
Mahieu, R. L. P., Borocz, I. M., & De Hert, P. (2021). *D2.2 Report on best practices: How national associations of DPOs can best support collaboration and communication through digital collaborative platforms, and structure the interaction between DPOs and the supervisory authority.*

Copyright

No part of this publication may be reproduced or transmitted in any form, without the prior written permission of the author(s) or other rights holders to whom publication rights have been transferred, unless permitted by a license attached to the publication (a Creative Commons license or other), or unless exceptions to copyright law apply.

Take down policy

If you believe that this document infringes your copyright or other rights, please contact openaccess@vub.be, with details of the nature of the infringement. We will investigate the claim and if justified, we will take the appropriate steps.



D2.2 Report on best practices

How national associations of DPOs can best support collaboration and communication through digital collaborative platforms, and structure the interaction between DPOs and the supervisory authority

René Mahieu
István Böröcz
Prof. dr. Paul de Hert
LSTS VUB

Table of Contents

1) Introduction.....	2
2) Method.....	2
3) Background.....	3
4) Findings.....	4
4.1) Relationship DPO-DPO.....	4
4.2) Best Practices DPO-DPO.....	4
4.3) Relationship DPO-SA.....	5
4.4) Best Practices DPO-SA.....	6
5) Conclusion.....	7
Bibliography.....	9

1) Introduction

The DPO-Connect project is a collaboration between the Belgian Supervisory Authority, the Research Group on Law, Science, Technology & Society (LSTS) of the Vrije Universiteit Brussel (VUB), and DPO-Connect, a Professional Association of Belgian Data Protection Officers. The goal of the project is to connect the community of Data Protection Officers (DPOs) and other privacy professionals with each other, and with the Belgian Supervisory Authority (SA), through a digital General Data Protection Regulation (GDPR) collaboration platform.

This report provides an overview of “best practices” of how national associations of DPOs can best support collaboration and communication through digital collaborative platforms, and structure the interaction between DPOs and SA. It is part of Work Package 2 “Setting up the requirements for the GDPR collaborative platform” and reviews the state-of-the-art in collaborative platforms existing in other EU Member States. The findings of this report will help in defining the structure and requirements of the platform that will be built in the context of the DPO-Connect project, but are also meant to support more generally the development of modes of communication and collaboration between DPOs and SAs in Europe, thereby contributing to a more effective implementation of the GDPR.

2) Method

This report is primarily based on interviews with representatives of DPO organizations and SAs, and supplemented by a review of the academic and professional literature on DPOs and in particular their relation with the SAs. We interviewed 10 people, 5 representatives of DPO organizations and 5 representatives of SAs.

To select the representatives of DPO organizations to interview, an inventory was made of the existing professional organizations of DPOs. This search resulted in a list of 23 such organizations. Among the DPO organizations, we selected those organizations that have existed the longest, and those we knew made use of a digital infrastructure to support their collaboration. We selected and spoke to representatives of Association Française des Correspondants à la protection des Données à caractère Personnel (AFCDP) in France, het Nederlands Genootschap van Functionarissen voor Gegevensbescherming (NGFG) in the Netherlands (established in 2003),¹ Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) in Germany, DPO-Pro in Belgium and the Network of Data Protection Officers appointed by the EU institutions and bodies. The two most elaborate digital infrastructures we encountered for collaboration were by AGORA,² a private social network run by AFCDP since 2011, and Datenschutz-Wiki,³ a specialized platform to gather data protection knowledge, also initiated in 2011.

We found representatives of national SAs by submitting a request for participation via the European Data Protection Board (EDPB). We interviewed representatives of the Belgian, Dutch, Estonian, Irish, Norwegian SAs as well as the European Data Protection Board (EDPB).

¹ <https://www.ngfg.nl/>

² <https://agora-afcdp.jamespot.pro/>

³ <https://www.datenschutz-wiki.de/Hauptseite>

The interviews were semi-structured interviews, lasting on average 45-60 minutes each and were conducted in May and June 2021. The interviews started from a basic set of questions to steer the conversation in a general direction, but had ample room for developing specific topics that came up in the individual conversations. Questions focused on the experiences with different modes of communication among DPOs, and in particular on the use of digital platforms in supporting this communication. We also asked about the interaction between DPOs and SAs and the role that the DPO associations play in this interaction.

3) Background

The data protection officer has an important role in the General Data Protection Regulation (GDPR). According to the EDPB the DPO “is a cornerstone of accountability [...] In addition to facilitating compliance through the implementation of accountability tools (such as facilitating data protection impact assessments and carrying out or facilitating audits), DPOs act as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation).”⁴

The role of the Data Protection Officer is, to a large extent, new. The Data Protection Directive (DPD) did have a small role for data protection officials. Only some EU member states regulated the role of data protection official in their national implementation of the DPD, and in most cases designation of a DPO was optional.⁵

According to Article 39(1)(e) GDPR the DPO has “to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.” This has been interpreted in opposing ways in the legal literature: Some authors interpret this as a duty on the SA to provide upon request consultation to the DPO, while others argue that this entails an obligation on the DPO to provide upon request consultation to the SA.⁶ The nature of the relation between the SA and the DPO is not specified further in the GDPR. Among the tasks of the SA, specified in Article 57 GDPR, the DPO is not specifically mentioned. However, given the general task of the SA, of monitoring and enforcing the application of the GDPR, and the general tasks of the DPO defined in Article 39 GDPR, it stands to reason to see them as natural allies.

As a consequence of the recent emergence of the role of DPO and the limited specification of its role in the GDPR, the way the role of DPO can best be fulfilled, as well as its position within the general architecture of the GDPR, is not yet settled. Yet, the effectiveness of the GDPR in practice depends crucially on the effective interaction between the various actors that are part of the Regulation’s “architecture of empowerment”.⁷ The professional organizations of DPOs established for DPOs to mutually support each other in most member states can play an important role in this

⁴ Article 29 Data Protection Working Party (2017), p4.

⁵ Gelly (2012).

⁶ Drewes (2019), p.908 and references therein. A quick look in the legislative history provides no clear indication as to which interpretation is correct. The initial proposal by the European Commission while worded slightly different is also ambiguous. The fact that the support to DPOs is not mentioned under tasks of the SA in Article 57 seems to favor the interpretation that there is no obligation on the SA to give consultation to DPOs, outside of the the framework of Article 36.

⁷ Mahieu and Auloos (2020), especially paragraph 23.

regard. The effectiveness of the position of DPOs, within the architecture of the GDPR, also depends on how their relationship with Supervisory Authorities (SA) is shaped.

4) Findings

This section first presents the general findings and best practices that relate to communication and collaboration among DPOs. It discusses how communication and collaboration between DPOs can strengthen their position, irrespective of the interaction with and support of the SA. In the second part the communication and relationship between DPOs and SAs is discussed.

4.1) Relationship DPO-DPO

The introduction of an obligation to appoint a DPO under certain situations has resulted in a quick rise in the number of DPOs in a very short time. This is the case in particular for countries such as Belgium, for which there was no obligation to appoint a DPO in the national implementation of the DPD. But it is also true for countries in which such an obligation already existed, because in most cases the conditions under which a DPO was obligatory have been broadened.

As a consequence of the quick rise in the number of DPOs, the level and type of experience of the people exercising this function differs greatly, as many people with relatively little experience in data protection have entered the profession.

Among organizations of DPOs, the topic of facilitating communication between DPOs is high on the agenda. For most organizations physical meetings were the main means of communication, but as these were not possible during the Corona pandemic, the use of digital communication platforms, for example through the hosting of seminars, has increased. Multiple organizations of DPOs are in the process of building platforms to facilitate cooperation among DPOs, and all contacted organizations expressed interests in learning from the results of the DPO-Connect project.

4.2) Best Practices DPO-DPO

Build a digital platform for collaboration among DPOs.

Both DPOs and SA experienced that any form of structured collaboration between DPOs is positive, and support the functioning of DPOs. This is particularly important given the fact that the DPO is a relatively small part of the organization, and there are few others in the organization that can function as impartial sounding-board. Feedback from peers can help strengthen the position of the DPO. Those who already used a digital infrastructure to support collaboration found that it was beneficial, and most of those who did not yet use it had high expectations for its possible use.

Foster trust among participants (it is a prerequisite for collaboration).

A digital platform can facilitate communication and collaboration in an existing community, but it is unlikely that the mere existence of a digital platform will create a sense of community. In order for people to be willing to put effort in contributing to a platform, it is helpful that they know each other in real life. All representatives of DPO associations reported that the organization of physical meetings is conducive to building trust among members, and that such meetings are appreciated by members. People need to be able to look each other in the eye. A basis of trust needs to be already there or else it needs to be built up.

Facilitate sector-specific collaboration.

Organizations that operate within a specific sector often have similar ways of processing personal data. Therefore, DPOs within a specific sector often get confronted with similar compliance questions.

Many professional organizations of DPOs provide opportunities for DPOs from specific sectors to meet and exchange experiences. The experience of AFCDP shows that within digital platforms organizing communication channels by sector has good results, and that engagement is relatively high. Similarly, in the offline context, several organizations of DPOs reported that sector oriented sub-groups functioned very well.

Dedicate resources to populate and moderate the platform.

Even when a platform is designed and meant for a community to produce and share content, practice shows that their success often depends on a small number of highly active contributors. Moreover, the usefulness of a platform to new users is dependent on the level of activity on the platform: When responses come pouring in quickly after a question is posed, it is useful to the user. When there are no reactions, or when reactions only appear after a long time, users will be disappointed, and may not return to the platform again. It is therefore crucial that, especially when a platform has just been launched, the initiators of the platform make sure that a core group of active users is present to animate discourse on the platform.

The platform needs to be moderated. The more open the platform is, in terms of whether and how members can contribute posts, start new threads or invite new members, the more moderation is needed. Moderation is needed to retain an organized structure of the information on the platform, for example by making sure that threads that discuss the same topic are merged. Moderation is also needed to make sure the platform remains open to all members and a plurality of voices.⁸

Do not unnecessarily duplicate efforts

It is the experience of existing platforms that it can be tempting to over-include additional resources into the platform. One association of DPOs for example, started working on a database of SA enforcement decisions, but eventually discontinued the effort. It found that maintaining the database involved considerable effort, and that it was hard to get the database up to date and complete. At the same time, it found that members preferred to use an existing database (www.enforcementtracker.com). In such cases best practice is to revert to the primary source, and if possible contribute to the primary source.

4.3) Relationship DPO-SA

The GDPR does not provide detailed instructions on how these two actors should relate to each other, and in particular whether and how the SAs should support the role of DPO. While the GDPR has a clear provision that SAs must support data subjects by providing information about their rights and handling their complaints,⁹ no similar provision exists regarding DPOs. This seems to have resulted in a disparity between the expectation on what support the DPO can expect from the SA: All but one interviewee working for SAs expressed the opinion that the SA does not have a legal obligation to support DPOs, while many members of DPOs thought such an obligation did exist. Nevertheless, SAs and DPOs generally agree that a strong relation between them would

⁸ Grimmelmann, 2015.

⁹ Article 57(1)(e-f) GDPR.

benefit the overall effectiveness of the GDPR. They also think, however, that many of the common practices of interaction between them are not satisfactory.

The most common form of communication between authorities and SAs is through one way communication via websites, frequently asked questions, seminars, position papers, and two-way communication via telephone, webform, post or email. However, as SAs have limited resources,¹⁰ and individual two-way communication is costly, the availability of individual help is often restricted. It is common practice that help-lines are only open during certain parts of the day,¹¹ and some SAs do not offer any help-lines.¹²

Moreover, most DPOs as SAs reported that responses to individual questions are often quite generic. As a general rule, SAs do not provide concrete advice about specific cases. The Dutch SA for example, states specifically on its website that it “answers questions from DPOs by explaining certain privacy standards and their general application”, and they “rarely pass judgment on a specific situation”.¹³ While DPOs generally do understand the position of the SA, this does lead to dissatisfaction on their part, and severely limits the perceived usefulness of hotlines.

Two main causes seem to underlie the perceived problems: The limited resources of the SAs, and the unequal expectations about the nature of the relationship between DPO and SA.

The SAs are often small, relative to other authorities such as financial market authorities, while the scope of their work is much wider. As a consequence, they are less specialized with regards to the various sectors they have to supervise.

Multiple SAs are currently re-assessing how they should relate to DPOs. In these assessments, reflections on the modes of communication play an important role. Consequently, there is a wide interest in understanding whether and how communication and collaboration platforms could contribute to improving the interaction between DPOs and SAs.

4.4) Best Practices DPO-SA

Using the platform as a filter for SA.

A centralized communication and collaboration platform can function as a filter for the SA to receive questions of common concern or ambiguity. In multiple member states, organizations of DPOs already function as an intermediary to bring issues of common concern to the attention of the SA. To this end, it is common practice for representatives of DPO organizations to have a meeting with the SA at fixed time-intervals (for example four times per year).

¹⁰ In the Netherlands for example, independent research found that the supervisory authority should more than double in size in order to be able to properly perform their statutory duties. Autoriteit Persoonsgegevens, Jaarverslag 2020, p.17. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2020.pdf

¹¹ The dedicated phone-line by the French SA is open days a week 2 hours per day (<https://www.cnil.fr/fr/contacter-la-cnil-standard-et-permanences-telephoniques>), that of the Norwegian SA 2,5 hours a day (<https://www.datatilsynet.no/om-datatilsynet/kontakt-oss/>), and that of the Dutch SA 3 hours a day (<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/functionaris-gegevensbescherming-fg#hoe-kan-ik-als-fg-de-ap-eeen-vraag-stellen-over-privacy-7147>), these practices were also mentioned by some of the interviewees.

¹² The Irish SA does not offer a help-line dedicated to DPOs.

¹³ <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/functionaris-gegevensbescherming-fg>.

A digital platform can support this function as it can allow DPOs to raise issues in a simple manner, and, through interaction among DPOs, it can become clear whether an answer to the question is available in the community. An added benefit is that the use of such a tool adds transparency to the process, as the questions raised, as well as the responses to the question can be seen by anyone with access to the platform. If the platform becomes a single point of access for DPOs to raise questions to SA, it would be important that the platform is accessible to all DPOs.

Formalizing the role of the SA on the platform and communicating clearly about it.

DPOs experience an intrinsic conflict in sharing information about specific processing operations with the SA, as enforcement of the GDPR is one of the main tasks of the SA. If DPOs share information to receive advice they inadvertently bring the authority's attention to potential infringements. It is therefore important to make a clear decision on how information from advise can be used by the SA. In response to this tension, one solution is to not invite the SA on the platform.¹⁴

In order to further safeguard the ability to discuss freely among DPOs, confidentiality of information exchanged between DPOs on the platform should also be guaranteed. Some DPO organizations have confidentiality agreements in their general codes of conduct, but it can also be part of specific terms and conditions for using the platform.

SA can empower the DPO by setting clear and specific standards

Concrete standards set by the SA help strengthen the position of the DPO within the organization. The GDPR is structured around general principles, and applying it in specific situations requires judgment and balancing of different interests. Concrete guidance by SAs help DPOs in at least two quite distinct ways. First, the guidance can provide clarity in situations that are complex, and where the weighing of interests and risks is not self-evident. Secondly, even when the application of the GDPR in a specific situation is clear from the perspective of the DPO, having concrete statements by the SA help strengthen the position of the DPO by limiting the margin of doubt about the validity of their position.

Multiple DPOs indicated that they would be very much supported in their position by more active enforcement by the SA. Contrary to the lack of specificity in their responses to questions posed through hot-lines, SAs do pass specific judgment on specific situation in decisions that it is taking in its capacity as enforcer. Therefore, enforcement decisions can function as a valuable resource for DPOs, which can also be disseminated and help inform discussions on online collaboration platforms. An additional benefit is that enforcement decisions also strengthen the position of the DPO by increasing the risk (expected cost) of non-compliance on the part of controllers and processors.

¹⁴ As is the case with the AGORA platform run by the AFCDP in France, where the CNIL is not on the platform. This also prevents the platform of getting to much of a privileged status.

5) Conclusion

Our interviews show that representatives of DPO organizations and SAs see the DPO as a key actor within the regulatory architecture of the GDPR. It is widely agreed upon, that the effectiveness of the DPO depends on the relationship between DPOs and SA, and the support of the DPO by the SA. At the same time, however, the way in which SAs should relate to DPOs is not at all settled. Moreover, many current common practices are perceived to be problematic: the cost for the SA is high, while the usefulness for DPOs is low.

Experience shows that digital and non-digital structures of collaboration and communication between DPOs can play a significant support function for individual DPOs, thereby decreasing the need for individual support by SAs as well as helping them to target their effort in a more efficient manner. This report identified a series of best practices. These best practices should be duly considered in developing collaborative platforms, such as the DPO-Connect platform. For example, such platforms should preferably include sectoral subgroups on the platform, a clear protocol for the about the confidentiality of the information shared by DPOs on the platform. And, in light of the need for dedicated resources to moderate and populate the platform a continuity plan should also be created.

Three best practices stand out to generally improve the interaction between DPOs and SAs, irrespective of whether a digital platform is used. First, facilitating communication between DPOs is generally effective in supporting DPOs, especially when DPOs that face similar problems are brought together, in particular through sectoral groups or by nature of their employment relationship. Second, digital infrastructure can play an important role in facilitating communication, but they should be grounded in other forms of connection. In other words, technological tools are not by themselves a solution. Third, collaboration platforms between DPOs should act as an effective filter for SAs to efficiently find and respond to problems that are perceived by multiple DPOs and for which no clear solution exists. To this and a protocol should be developed to regulate how questions raised on the platform can reach the SA.

Bibliography

Alvarez Rigaudias, Cecilia, and Alessandro Spina. “Article 37 Designation of the Data Protection Officer.” In *The EU General Data Protection Regulation (GDPR) -- A Commentary*, edited by Christopher Kuner, Lee A. Bygrave, Christopher Docksey, and Laura Drechsler, 688–99. Oxford: Oxford University Press, 2020.

Article 29 Data Protection Working Party. “Guidelines on Data Protection Officers (‘DPOs’).” Brussels, April 5, 2017.

Drewes, ‘Artikel 39’ in Spiros Simitis, Gerrit Hornung and Indra Spiecker (eds), *Datenschutzrecht DSGVO mit BDSG* (1st edn, Nomos Verlagsgesellschaft 2019)

Gelly, Pascale. “Comparative Analysis of Data Protection Officials Role and Status in the EU and More.” Confederation of European Data Protection Organisations, February 2012.
https://www.gdd.de/downloads/materialien/internationales/DPO_Spreadsheet_All_Countries.PDF.

Grimmelmann, J. (2015). The Virtues of Moderation. *Yale Journal of Law and Technology*, 17(1), 42–109. <https://doi.org/10.31228/osf.io/qwxf5>

Mahieu, R., & Ausloos, J. (2020). Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access. *LawArXiv*. <https://doi.org/10.31228/osf.io/b5dwm>