




The Data Protection Officer: A Ubiquitous Role That No One Really Knows

Francesco Ciclosi  | University of Trento

Fabio Massacci  | University of Trento and Vrije Universiteit Amsterdam

Versed in legal, management, and cybersecurity technical skills, the data protection officer stands between those auditing a company's compliance and those acting as management advisors. We describe how this role tackles sociotechnical risks in everyday scenarios.

The recent application of Regulation (EU) 2016/679, better known to the world as the *General Data Protection Regulation (GDPR)*, introduced the role of the data protection officer (DPO). Although DPOs have been a key enabler of the GDPR,³ the role of this privacy worker is not a new concept: in several European Union (EU) member states, its appointment was already good practice for some years. Yet, the GDPR does not formally describe the DPO job profile, and many papers discuss how to support a DPO with algorithms without providing practical examples of what the DPO does.

For example, Diamantopoulou et al.⁴ identify which ISO 27001/2 controls need to be extended to meet GDPR requirements and which of them the DPO is involved, but why in some and not in others? Ryan et al.⁵ explain how their framework RegTech can be helpful to a DPO for checking GDPR compliance, but when and for what concretely? Chatzipolidis et al.⁶ describe a readiness assessment tool for GDPR's compliance, but for solving social or technical issues? Other

articles discuss GDPR's compliance topics as if DPOs did not exist, from software engineering⁷ to socio-technical management processes,⁸ or the GDPR's cost among cybersecurity investments.⁹

Our purpose is to introduce this legally required organizational role—this ubiquitous privacy worker—to the engineering community, represented by *IEEE Security & Privacy Magazine* readers, through concrete examples of what problems DPOs face, what they do, and what they may or must know. Although the literature is surprisingly silent on this, we think that knowledge of the everyday challenges that DPOs have is the starting point for all subsequent research activities. For example, if a researcher has no reference to the daily activities of the key privacy worker in charge of GDPR compliance, how can one design logic or a tool for checking this privacy compliance or any privacy-by-design technology with a practical impact? In summary, the following is our key research question: Can we enucleate, in a few representative scenarios, the concrete activities of a DPO?

The article focuses on the role of the DPO introduced by the GDPR, but the insights are valuable for readers outside EU countries. The GDPR can apply to organizations that carry out their activities in the EU

Digital Object Identifier 10.1109/MSEC.2022.3222115
Date of current version: 22 December 2022

and organizations outside the EU that process the personal data of EU data subjects. Further, in many countries worldwide, there is data protection legislation in which a DPO role exists at some level. The International Association of Privacy Professionals lists the different roles in many countries worldwide that share some characteristics with the DPO legally defined in the EU (https://iapp.org/media/pdf/resource_center/dpo_requirements_by_country.pdf).

Our Methodology

The insights described in this article are grounded in case studies along Yin's case study methodology^{2,Ch.4} and the suggestions by Glaser and Holton,¹⁶ with the former being the founder of grounded theory, to build core categories across field observations derived from the live experience.

First, we analyzed data protection laws and recommendations from relevant authorities. Second, we analyzed the seven functions of the DPO that the European Data Protection Supervisor (EDPS) identified in its paper on the role of the DPO in compliance with Regulation (EC) 45/2001. Then, we looked at the summary of opinions of some supervisory authorities (SAs) (i.e., Bulgaria, Croatia, Italy, Poland, and Spain) on the DPO's activities involved with these functions (e.g., in the work of Korff and Georges¹) to have a perspective that was not restricted to a single country.

To make this article concrete as a use-case reference, we selected only sources of information for which there was evidence that the activities carried out by the DPO involved at least one of these seven functions. The starting point for the case study selection was the personal experience of the first author, who has been a DPO in the Italian public administration for the past five years and is a member of the Italian Association of DPOs.

To make the results of our study accessible, we looked for some publicly available information (for example, court decisions, SAs' decisions, and newspaper articles) on case studies similar to the ones on which the first author had firsthand experience. This approach allows us to go beyond the individual experience and provide shareable evidence. Out of more than 90 public case studies, we finally distilled 12 scenarios with at least one analyzable practical example for each of the

DPO's primary functions. In this article, we made the scenario general by renaming the actors involved (but without altering their nature) to be resilient to potential requests on the "right to be forgotten" and be of general interest to the reader.

The scenarios we propose map well into the general literature. For example, the <https://www.enforcementtracker.com/> website reports 1,475 occurrences of GDPR fines related to DPOs across 31 different EU Member or European Economic Area States. Our scenarios cover more than 1,400 cases.

How This Role Was Born

In Europe, the DPO concept came from the German Federal Data Protection Act of 1977, the Bundesdatenschutzgesetz, which introduced a precursor of the role (see Figure 1).

Over time, the DPO role became widely adopted by other European countries until, in 1995, the European Community issued Directive 95/46/EC on the protection of individuals

concerning the processing of personal data and on the free movement of such data. A patchwork of approaches followed: many member states introduced the DPO role in their national law, like in Austria (where the appointment was mandatory) or France (where the

appointment was optional), but only some of them (in Italy, the DPO role was absent in national law). Moreover, DPO duties were limited to independently ensuring an organization's internal application of the national provisions taken according to the Directive and keeping a register of processing operations carried out by the controller.

For EU institutions, only the appointment of at least one DPO was mandated by Regulation (EC) 45/2001. These rules were very similar to the ones that would be introduced in later years. The year 2016 was a pivotal year for data protection as the European Parliament and the Council issued Directive (EU) 2016/680 on criminal offenses or criminal penalties, and the GDPR on personal data protection.

To provide an interpretation of the EU's data protection legislation, the Article 29 Working Party Committee issued the Guidelines on DPOs (WP243),¹⁰ which was initially adopted on 13 December 2016, and later revised on 5 April 2017. After GDPR adoption, the new European



In summary, the following is our key research question: Can we enucleate, in a few representative scenarios, the concrete activities of a DPO?



Data Protection Board (EDPB), an independent European body tasked with ensuring the consistent application of data protection rules throughout the EU, endorsed these guidelines in its first plenary meeting on 25 May 2018.

Not all organizations are required to appoint a DPO, although doing so is good practice. There are three specific cases in which a controller or a processor must appoint a DPO (GDPR, Article 37). In the first case, if the organization is a public institution, it must appoint a DPO. Otherwise, an organization must appoint a DPO if it requires regular and systematic monitoring of data subjects on a large scale (second case) or processes, on a large scale, personal data that belong to special categories or are related to criminal offenses (third case).

Article 39 of the GDPR entrusts the following different tasks to a DPO:

- informing and advising one’s employer, who is carrying out the processing, of its obligations under the law
- monitoring compliance with the law
- providing advice regarding the data protection impact assessment (DPIA) and monitoring its execution
- cooperating with the SA as a contact point between this and the organization.

Table 1 summarizes the seven functions of the DPO, identified by the EDPS in its position paper on this role.

In summary, DPOs must be fully cognizant of the controller’s working environment to carry out their tasks. This awareness implies that a DPO must know the internal distribution and allocation of the responsibilities and tasks related to every personal data processing activity. A DPO must also be familiar with any external links (between the controller and other organizations) and with legal frameworks in which these links take place. According to many SAs’ opinions,¹ a preliminary task in which a DPO scopes the controller’s environment fulfills this requirement.

What Problems Does a DPO Face?

To understand the daily problems a DPO faces, we illustrate several real-life scenarios in Table 2. We edited them to obfuscate the original entity responsible for the privacy issues faced by the DPO. The supplemental material, available at <http://arxiv.org/abs/2212.07712>, reports the sources of these scenarios.

Empirical research on the problems of DPOs¹¹ has shown that sometimes these could be very basic and relate to a lack of sufficient resources (time, finances, and humans) to carry out one’s duties, and to some issues in the operational interpretation of the law. In Table 2, we analyze the challenges that DPOs face even when adequately supported.

For example, although maintaining a record of processing activities is formally a controller’s duty, the

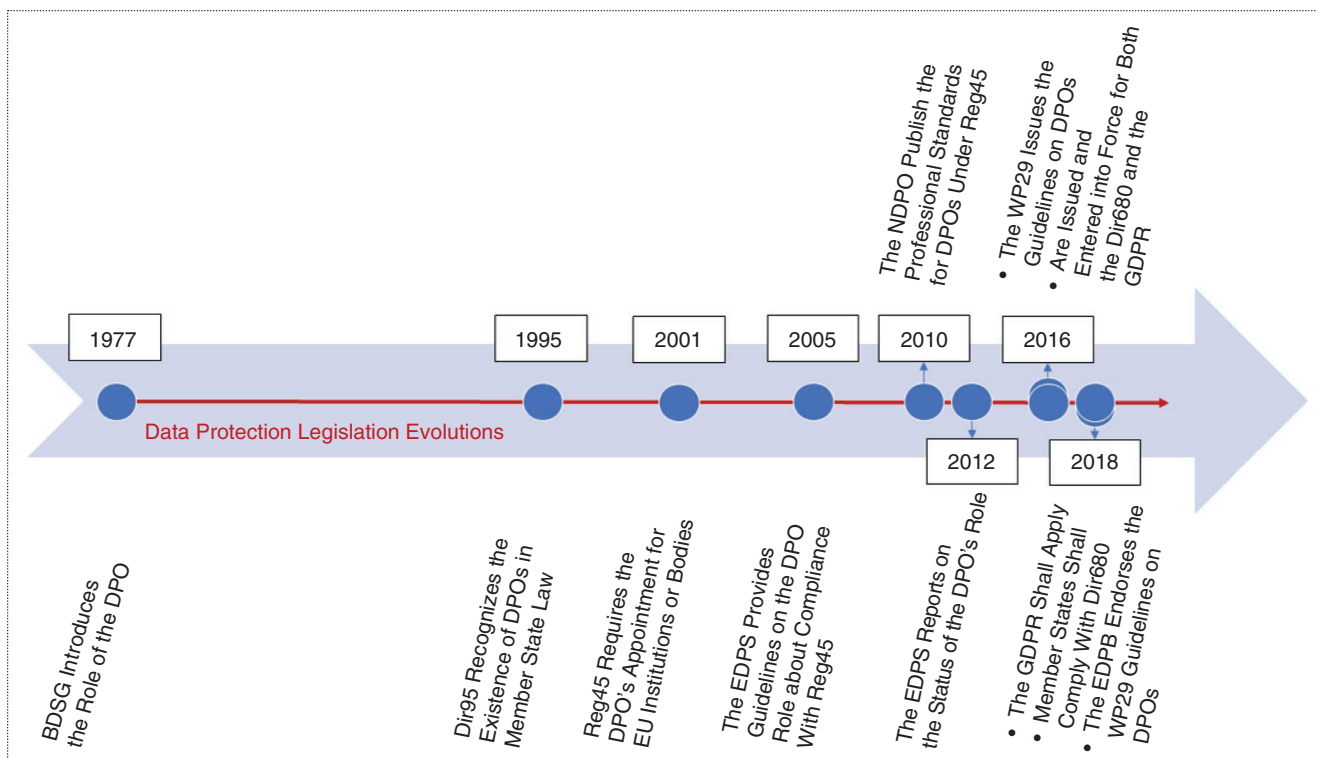


Figure 1. Evolution of the European role of the DPO. BDSG: Bundesdatenschutzgesetz; NDPO: Network of Data Protection Officers.

DPO will most likely be in charge of this work or closely involved in its oversight activities. In some job advertisements for DPO appointments, it is formally stated that the DPO is in charge of maintaining a record of processing activities. Without a regulatory constraint, the DPO may also be appointed to carry out some activities that are formally a duty of the controller. It is the controller's choice who pays the DPO. The involvement of the DPO is only sometimes an indicator that things are working well. A data controller could use a non-GDPR-compliant service because of a DPO's mistake (see "WRONG-ADVICE" in Table 2). Unfortunately, the controller is solely responsible for the choice made, and even a DPO's evaluation errors expose it to administrative fines or penalties. The accountability principle constrains the controller to demonstrate having complied with the regulatory requirement.

In an opposite scenario, a controller operating a catering service implements a new data processing activity to control the EU Digital COVID Certificate of staff but neglects the DPO's advice without justifying in writing why that advice has not been taken into account (the "IGNORED-DPO-ADVICE" scenario). This action is to blame because it is reasonable that the DPO gave his or her advice to ensure that the processing complied with the GDPR. Again, not documenting the reasons behind choosing to neglect this advice results in violating the accountability principle, exposing data subjects to risks and the controller itself to administrative fines or penalties.

The DPIA execution is a controller's responsibility, while the DPO task is limited to providing the advice

requested. The WP29¹⁰ highlights that a controller should clearly justify in the DPIA's documentation why it has not considered the DPO's advice. For properly handling the execution of a DPIA, a controller could define, in an internal regulation, the procedures for consulting the DPO about this topic. By way of example, this regulation may contain whether or not to carry out a DPIA, what methodology to follow, and whether to use internal resources or outsource it. Other helpful information to include in the regulation is which safeguards to apply to mitigate any risks to the rights and freedoms of the data subjects.

The "DPO-ADVICE-NOT-SOUGHT" scenario describes a case in which a controller is exposed to mistakes in the processing's design because it did not request the DPO's advice. The "WEBSITE-FORCES-CHOICES" scenario exemplifies the vulnerability stemming from the wrong implementation of a transport company's seat reservation software procedure. The software forced the data subject to consent to other forms of processing.

The "ADMIN-ASKS-FOR-EVERYTHING" scenario is related to a failed application of the minimization principle. In it, the human resources office of a public institution (which must satisfy the law on publication obligation) publishes the unredacted curriculum vitae of the winner of a public selection in the "Transparent Administration" section of the institution's website, thus exposing the data subject's personal data (e.g., the home address, personal phone number, and so on).

The relationship between the DPO and the SA is significant. The WP29¹⁰ highlights that the DPO must act as a "facilitator" by cooperating with the SA.

Table 1. A high-level view of the functions of DPOs. This table describes the tasks of the DPO, grouped according to the seven functions of the DPO that the EDPS identified in its position paper on the role of the DPO in compliance with Regulation (EC) 45/2001.

DPOs' functions	Summary descriptions
Organizational function	Review or even directly organize a processing operations register on behalf of the controller, help both assess the related risks, and support the processing activities with high-risk value
Monitoring of compliance	Investigate (on autonomous initiative) matters and occurrences directly related to the GDPR, and report back to the controller
Advisory function	Make recommendations for the practical improvement of data protection to the controller, and advise it on matters concerning the related provisions
Cooperative function	Facilitate cooperation (between the SA and the controller), especially in the frame of investigations, complaint handling, or prior checks
Handle queries or complaints	The authorization to handle queries or complaints originated from the very possibility of autonomous investigations
Information and raising-awareness function	Prepare staff information notes, training sessions, privacy statements, and learning material
Enforcement	Powers of enforcement are limited

Furthermore, the obligation of secrecy or confidentiality cannot prohibit the DPO from contacting and seeking advice from the SA. The controller who acts to weaken this relationship could be sanctioned. If the data controller does not appoint the DPO, problems will likely arise in the “NEGLECTED-SUBJECT-RIGHT” and “SUBJECT-RIGHT-REQUEST” scenarios. In the “NEGLECTED-SUBJECT-RIGHT” scenario, another

violation is the missing communication to the SA of the DPO’s contact details because, in that case, the SA does not know how to contact the DPO to handle the complaint. In the “SUBJECT-RIGHT-REQUEST” scenario, an aggravating factor would occur if, when the controller draws up the record of processing activities, it does not correctly identify them. In such a case, even if appointed, the DPO may find it challenging to identify

Table 2. The scenarios and privacy issues faced daily by a DPO.

Short name	Scenario description	What went wrong
WRONG-ADVICE	A controller wants to process data using a processor service and asks the DPO’s advice to understand whether the proposed contract complies with the GDPR.	The advice of the DPO turned out to be wrong, but the controller uncritically trusted the DPO’s advice.
IGNORED-DPO-ADVICE	A controller implements new data processing. The DPO advises that previous execution of a DPIA is required.	The controller chooses to neglect the DPO’s advice without justifying in writing why it did not take into account that advice.
DPO-ADVICE-NOT-SOUGHT	A controller implements a registration procedure of service without prior asking for the DPO’s advice about compliance with GDPR principles.	The registration procedure does not carry out a check on the identity of the person who enrolls, so it is unknown who saw the data.
WEBSITE-FORCES-CHOICES	In a controller procedure, data processing for marketing purposes asks for the consent of the data subject.	The procedure forces a data subject to release consent, imposing him or her to select a box, otherwise preventing it from continuing.
ADMIN-ASKS-FOR-EVERYTHING	A controller’s staff member satisfies the law on access to data (e.g., the Freedom of Information Act) by publishing some documents about a data subject.	A controller processes personal data by asking the data subject and publishing all data without correctly applying the data-minimization principle.
NEGLECTED-SUBJECT-RIGHT	A data subject files a complaint with the competent SA because he or she has not received a response within the time frame set by law.	The controller did not designate the DPO, or it did, but the designated DPO did not monitor the official address.
SUBJECT-RIGHT-REQUEST	A data subject exercises one’s rights of access according to Article 15 of the GDPR, sending a formal request to the DPO’s address.	When the controller drew up the record of processing activities, it did not correctly identify the actual processing activities, so the DPO could not answer the query.
NO-DATA-PROTECTION-PRINCIPLES	A controller implements a configuration in company equipment.	There is an incorrect configuration that allows unfettered access to personal data.
UNCHECKED-REMOTE-MONITORING	A controller implements remote assistance software tools on company workstations.	The technicians use a remote assistance software solution that does not notify the user when remote access is performed.
WRONG-PUBLIC-PROCUREMENT	A controller issues a public tender for procuring products or services.	In the tender evaluation grid, there is no explicit checkpoint for applicants to “demonstrate” that their products or services fully comply with the GDPR.
SOFTWARE-END-OF-LIFE	The DPO of a company noticed some results about the software used for processing activities.	The software used in the company’s workstations is obsolete, and the support provided by the vendor’s software house is expired or close to expiring.
SUBCONTRACTOR-VIOLATES-PRIVACY	A controller appoints its DPO to test the software procedure of a tender’s winner.	The tender winner has violated the contract for the supply of IT program and service terms on GDPR compliance.

the processing details and promptly respond to the data subject's requests.

Risk Management

DPOs face many challenges that we can classify into two categories: technical and socio-organizational risks. The first challenge stems from faulty technical or technological solutions that do not fully guarantee the protection of subjects whose personal data are processed. The second type of challenge is due to incorrect organizational procedures or incorrect human behavior.

We can subdivide technical risks into two subgroups. The first type relates to design problems when the DPO supports and advises the controller on technical choices. For example, the DPO may be asked to choose between configurations that comply with the data-protection-by-default principle and configurations that seem to do so ("NO-DATA-PROTECTION-PRINCIPLES" and "UNCHECKED-REMOTE-MONITORING" in Table 2). He or she might find (or fail to find) insecure technical solutions in a call for tenders (the "WRONG-PUBLIC-PROCUREMENT" scenario) that can cause kick-start litigation between contractors. The second type of risk involves misconfigurations or errors that appear during implementation (the "SUBCONTRACTOR-VIOLATES-PRIVACY" and "SOFTWARE-END-OF-LIFE" scenarios).

Socio-organizational risk can appear daily while the DPO supports the controller in processing activities. We can divide them into the following four additional categories, as listed in Table 2: auditing ("IGNORED-DPO-ADVICE" and "SUBCONTRACTOR-VIOLATES-PRIVACY"), communication ("NO-DATA-PROTECTION-PRINCIPLES" and "UNCHECKED-REMOTE-MONITORING"), processing designing ("SOFTWARE-END-OF-LIFE"), and relationship ("NEGLECTED-SUBJECT-RIGHT"). Conflicting requirements are a particular instance of these risks.

No matter how sophisticated the technical protection measures are, DPOs may experience side-channel attacks from the most unexpected human behavior. A well-designed processing activity may become unlawful because a staff member operates differently from what is prescribed by the procedure and from the instructions received by the controller. For example, using a smartphone, an operator recorded the screen of closed-circuit video surveillance cameras, which was accessible only to the local police control station, and disseminated a video of a traffic accident on social media.

Table 3 shows some of the possible consequences of damaging the freedom and rights of natural persons. It is difficult to determine the impact grade without an in-depth analysis of the processing and the technical and organizational means used to mitigate their risks.

In some circumstances, the case study's high-level description (e.g., in the case of the GDPR accountability principle's violation) is sufficient to conclude that the consequences are actual and potentially disastrous for an organization. Because a personal data breach is a broad concept, we split this into three classes representing the specific breach. Finally, Table 3 includes some more specific classes (e.g., "GDPR-noncompliant processing" is a particular case of "unlawful processing").

Some DPO mistakes (such as "WRONG-ADVICE") may also cause a controller's wrong assessment, which subsequently induces wrong organizational choices.

If a threat exploits even one vulnerability, it will determine a GDPR's principles violation, exposing the controller to fines or penalties. Of course, this might depend on somebody tipping off the SA or the SA coming to investigate its initiative, or after a data breach.

What Does a DPO Actually Do?

The boundary between the DPO's functions is sometimes fuzzy, especially in complex scenarios where more of them are involved. In Table 4, we summarize some examples, presenting the role of a DPO in mitigating vulnerabilities (namely, prevention, detection, response, and investigation) for each scenario in Table 2.

In the "DPO-ADVICE-NOT-SOUGHT" scenario, the DPO's activities correspond to a detection ("D1" and "D2") and a response scenario ("R2," "R5," "R7," and "R10"). The DPO primarily exercises the monitoring of compliance. However, in the response part, there is a combination of the advisory, organizational, and cooperative functions, performed secondarily as well as the enforcement one.

The "WEBSITE-FORCES-CHOICES" case corresponds to two different scenarios. The first is a detection scenario in which the DPO exercises the function monitoring of compliance ("D1" and "D2"), while the second is a response one where the enforcement function is applied ("R5").

In the "ADMIN-ASKS-FOR-EVERYTHING" scenario, the DPO carries out his or her activities in a response scenario. Some ("R3" and "R9") combine enforcement and the handle queries or complaints functions. At the same time, another ("R11") primarily involves the handle queries or complaints function and, secondarily, the monitoring of compliance ones.

The importance of the DPO's cooperation function comes to light from the "NEGLECTED-SUBJECT-RIGHT" and "SUBJECT-RIGHT-REQUEST" scenarios. These cases are linked to two response scenarios. The first is involved primarily in the DPO's handling

of queries or complaints function, followed by the monitoring of compliance functions (“R11”). The second relates to handling queries or complaints and monitoring compliance function (“R4” and “R12”).

Moreover, related to the “NEGLECTED-SUBJECT-RIGHT” scenario, there is an additional response scenario in which the DPO’s cooperative function is primarily involved, which follows up on handling

Table 3. Some possible consequences of risks that a DPO may face. This table summarizes some examples of the consequences of technical or social risks that a DPO may face while carrying out his or her duties. These consequences are grouped into classes and associated with a possible reference scenario. Any such infringement exposes the controller to administrative fines of up to €20,000,000 or up to 4% of the total worldwide annual turnover, whichever is higher.

Impact class	Impact example	Scenario example
Attack on customers	Identity theft of the data subject could happen (e.g., an attacker steals a data subject’s personal data from a misconfigured database and later uses them, pretending to be the data subject).	NO-DATA-PROTECTION-PRINCIPLES, DPO-ADVICE-NOT-SOUGHT, IGNORED-DPO-ADVICE
Attack on employees	Unauthorized persons could capture the private data of employees.	UNCHECKED-REMOTE-MONITORING
Contract termination	It is possible that the tender could be subject to litigation due to a violation of the terms indicated in the contract for the supply of IT programs and services.	SUBCONTRACTOR-VIOLATES-PRIVACY
Data breach (access or disclosure)	A personal data breach may happen because of unauthorized access to (or disclosure of) personal data transmitted, stored, or otherwise processed (e.g., a software’s misconfiguration allows technicians to connect to a workstation without the user’s consent stealthily).	UNCHECKED-REMOTE-MONITORING, SUBCONTRACTOR-VIOLATES-PRIVACY, NO-DATA-PROTECTION-PRINCIPLES
Data breach (destruction or loss)	There is an unlawful destruction or accidental loss of personal data held by the controller (e.g., a malware type of ransomware has ciphered all the office’s files stored in a file server).	SOFTWARE-END-OF-LIFE
Data breach (alteration)	There is an unlawful alteration to personal data stored (e.g., exploiting a system’s vulnerability, a cracker modified some personal data stored in a database).	SOFTWARE-END-OF-LIFE, NO-DATA-PROTECTION-PRINCIPLES
Data disclosure	Excess and irrelevant personal data are disseminated over the Internet by the controller.	ADMIN-ASKS-FOR-EVERYTHING, NEGLECTED-SUBJECT-RIGHT
Inadequate identification	Anyone could pretend to be another data subject and access his or her personal data.	DPO-ADVICE-NOT-SOUGHT
GDPR-noncompliant processing	A controller processes personal data without providing information to the data subject (e.g., a controller issues a loyalty card to a customer without providing the customer with a privacy policy).	WRONG-ADVICE, IGNORED-DPO-ADVICE
Risky processing	The processing could be risky for the rights and freedoms of natural persons.	IGNORED-DPO-ADVICE
Unlawful processing	There is no legal basis for the processing. For example, the procedure forces the data subject to release consent for an unnecessary activity. In another example, a controller acquires personal data for one purpose and uses them for another purpose without obtaining the data subject’s consent.	WEBSITE-FORCES-CHOICES
Unlawful procurement	A contractor that offers non-GDPR-compliant products or services can win a bid. The call for the tender may be subject to litigation.	WRONG-PUBLIC-PROCUREMENT

Table 4. Some examples of the activities that a DPO carries out to mitigate consequences of realized risks.

ID	Illustrative mitigation by the DPO	Applicable scenarios (or DPO's function)
Prevention (P)—controller initiated		
P1	A group of joint controllers (two or more controllers who jointly determine the purposes and means of processing) asks their DPOs for advice on the technical and organizational aspects of periodic or new processing. For example, processing will build on an integrated territorial video surveillance system using optical character recognition cameras.	Advisory function, cooperative function, organizational function and monitoring of compliance
P2	The DPO helps the controller do a DPIA before starting new high-risk processing (e.g., one related to a COVID-19 screening data acquisition and management system).	Organizational function
P3	The DPO supports the controller with choosing the configuration of a company's telecommunication equipment or a software tool that guarantees the protection of personal data by default.	NO-DATA-PROTECTION-PRINCIPLES, UNCHECKED-REMOTE-MONITORING
Prevention—DPO initiated		
P4	A DPO monitors the data protection law changes and the indications of the bodies in charge, and after that, he or she prepares short information pills or notes for a small- and medium-enterprise (SME) staff.	Information and raising-awareness function
P5	The DPO advises the controller that in issuing public tenders, it should expressly call for applicants that can "demonstrate" that their product or service fully complies with the GDPR.	WRONG-PUBLIC-PROCUREMENT
P6	The DPO advises the controller to launch a census of all the PCs in the organization that have a Microsoft operating system version of 7 or older. The DPO interacts with the Information and Communications Technology department to develop an updated operating software plan.	SOFTWARE-END-OF-LIFE
P7	The DPO of a national central bank illustrates to some banks' DPOs the controller's obligations.	Advisory function
P8	The DPO consults with the competent SA about implementing new data processing.	Cooperative function
Investigate (I)—DPO initiated		
I1	The DPO initiates an investigative activity to verify compliance with contract terms.	SUBCONTRACTOR-VIOLATES-PRIVACY
I2	The DPO immediately advises the controller about the existence of a violation of the contract terms. The controller, in turn, immediately formally warns the processor about this violation, ordering it to stop the infringement at once (e.g., by returning the data encryption key).	SUBCONTRACTOR-VIOLATES-PRIVACY
Investigate—data subject initiated		
I3	A DPO receives a piece of informal information and initiates an investigative activity (e.g., to verify the control procedure of the EU Digital COVID Certificate held by the staff).	Monitoring of compliance and handle queries or complaints
Detection—DPO initiated		
D1	Examining the output of an audit, the DPO finds that the processing is not compliant with GDPR principles or is unlawful.	DPO-ADVICE-NOT-SOUGHT, WEBSITE-FORCES-CHOICES
D2	The DPO conducts periodic audits of processing compliance with GDPR principles.	IGNORED-DPO-ADVICE, DPO-ADVICE-NOT-SOUGHT, WEBSITE-FORCES-CHOICES
Response—controller initiated		
R1	The DPO could refuse to sign the GDPR compliance of a new or modified processing.	Enforcement
R2	The DPO assists the controller with investigating whether a personal data breach has occurred.	DPO-ADVICE-NOT-SOUGHT, SUBCONTRACTOR-VIOLATES-PRIVACY

(Continued)

Table 4. Some examples of the activities that a DPO carries out to mitigate consequences of realized risks. (Continued)

ID	Illustrative mitigation by the DPO	Applicable scenarios (or DPO's function)
	Response—DPO initiated	
R3	The DPO invites the controller to immediately remove irrelevant and excess personal data and apply the data-minimization principle.	ADMIN-ASKS-FOR-EVERYTHING, WEBSITE-FORCES-CHOICES
R4	The DPO interacts with the controller's structure to follow up on the data subject's request.	NEGLECTED-SUBJECT-RIGHT, SUBJECT-RIGHT-REQUEST
R5	The DPO advises the controller to immediately stop the processing by temporarily suspending the service to modify the software procedure.	DPO-ADVICE-NOT-SOUGHT, WEBSITE-FORCES-CHOICES
R6	After the controller follows up the data subject's request, the DPO reports it to the SA.	NEGLECTED-SUBJECT-RIGHT
R7	The DPO notifies the SA of a personal data breach, acting on behalf of the controller.	DPO-ADVICE-NOT-SOUGHT, SUBCONTRACTOR-VIOLATES-PRIVACY
R9	After the controller deletes irrelevant and excess personal data, the DPO notifies the data subject of complaint upholding.	ADMIN-ASKS-FOR-EVERYTHING
R10	The DPO communicates a data breach to the data subjects, acting on behalf of the controller.	DPO-ADVICE-NOT-SOUGHT, SUBCONTRACTOR-VIOLATES-PRIVACY
	Response—SA initiated	
R8	The DPO interacts with the SA, giving it the best collaboration in handling complaints lodged versus the controller and facilitating access to the documents and information.	NEGLECTED-SUBJECT-RIGHT
	Response—data subject initiated	
R11	The DPO checks whether the complaint or request received from the data subject is well founded.	ADMIN-ASKS-FOR-EVERYTHING, NEGLECTED-SUBJECT-RIGHT, SUBJECT-RIGHT-REQUEST
R12	The DPO responds to a data subject who applied for information about personal data processing, promptly providing all the requested information.	NEGLECTED-SUBJECT-RIGHT, SUBJECT-RIGHT-REQUEST

queries or complaints function (“R6” and “R8”). The “NO-DATA-PROTECTION-PRINCIPLES” and “UNCHECKED-REMOTE-MONITORING” cases highlight the importance of the DPO’s organizational function (“P3”), primarily in a prevention scenario. The advisory function follows up as second in the same.

In the “WRONG-PUBLIC-PROCUREMENT” scenario, there is an example of a prevention scenario in which the DPOs exercise their advisory function (“P5”). Although in the “SOFTWARE-END-OF-LIFE” scenario, there is a prevention scenario where DPOs exercise a combination of their organizational and advisory functions (“P6”). The “SUBCONTRACTOR-VIOLATES-PRIVACY” scenario shows the DPO’s monitoring of compliance use in an investigative scenario (“I1”). Then, in a combination of response and investigative scenarios, the DPO exercises the monitoring of compliance function, followed by a mix of the advisory, organizational, and cooperative functions performed secondarily (“R2,” “R7,” “R10,” and “I2”).

Regarding the DPO’s advisory function, when DPOs are involved in new data processing, they can consult the SA if necessary (“P8”). In the WEBSITE-FORCES-CHOICES scenario, when the DPO becomes aware of a process that is not entirely compliant with data protection policies (“D2”), he or she advises the controller, making recommendations for practically improving it (“D1,” and then “R3” or “R5”).

Finally, the DPO should perform the investigative activity even if the controller does not involve him or her. Foreexample, in the “SUBCONTRACTOR-VIOLATES-PRIVACY” scenario, the DPO can independently carry out this activity (“I1”). If he or she finds a violation of data-protection-by-design and default principles, the DPO acts accordingly (“I2”).

What Does a DPO Need to Know?

The GDPR does not specify the professional qualities required by a DPO, only that the necessary expert knowledge must be adequate for the data processing

operations and their protection rank. The WP29¹⁰ suggests that the required knowledge must be commensurate with the sensitivity, complexity, and amount of data the organization processes. Table 5 summarizes the expertise and skills that a DPO should have. They consist of qualities, expertise in law and practices, abilities, and educational qualifications.

In the absence of relevant bodies' specific guidance, from a legal perspective, it is challenging to define the DPOs' selection criteria that can truly measure the adequacy of their level of knowledge. Although technical and management skills are essential, there is no consensus on the "specific" certifications that guarantee a DPO's adequate expert knowledge level. As a result, it is difficult to establish the absolute value of specific qualifications (e.g., a master's degree), professional certifications (e.g., UNI 11697: 2017 certification), and being an author of books, articles, papers, or research products. The courts have reverted, as unfair requirements, several attempts to mandate different certifications (e.g., BS-7799 or ISO 27001).

In our experience, a DPO can achieve a good knowledge of data protection practices by studying documents arranged by the EDPB, EDPS, European Union Agency for Cybersecurity, and SAs of EU member states.

Another critical point is finding appropriate training for the professional profile of the DPO, both from a technical and a legal point of view: although knowledge of data protection law is a crucial requirement, a DPO may not have a law degree. A DPO may have a cybersecurity degree, but a European study¹² found that European master of science programs in cybersecurity do not practically cover the knowledge units on component procurement. Knowing this unit is critical to guarantee compliance with the privacy-by-design principle because third-party components and contracts with IT providers are the norms for any administration because they rarely have in-house developers.

Some training support can also come from internal and external information sources. An example of

Table 5. The expertise and skills of the DPO. This table describes the expertise and skills a DPO should have to carry out his or her tasks well.

Criteria	Description	Examples
Qualities	DPOs must possess specific professional qualities	SAs provide continuous training courses reserved for DPOs (e.g., the T4Data international project and the SME Data project). In the call for a DPO's appointment, a controller required that the candidates must have are in-depth knowledge of the organizational structure, the information systems present, and the specific sector of activity of the controller as well as being familiar with the data processing operations carried out by the latter. The EDPS asserts that it is better to recruit the DPOs of EU institutions/bodies/agencies (EUI) within the EUI. These people usually ensure a better knowledge of the organization, structure, and functioning of the EUI itself.
Expert in law	DPOs must have expert knowledge of data protection law	The EDPS asserts that the expert knowledge of data protection law is a prerequisite to the EUI's DPO function. In the call for a DPO's appointment, a controller required that the candidates must know are legislation and practices on data protection, both from a legal and IT point of view, including in-depth knowledge of the GDPR.
Expert in IT practice	DPOs must have expert knowledge of IT, security, and organization	According to the EDPS for EUI's DPOs, one of the professional qualities is knowledge of IT, including security aspects and organizational and communication skills. The Network of Data Protection Officers of the EUI recommends that the EUI's DPOs should have at least three years of relevant experience/maturity to serve as the DPO in a body where data protection is not related to the core business. Otherwise, this period grows to at least seven years. A similar thing happens if the DPO serves in an EU institution or that has an essential volume of processing operations.
Ability	DPOs must have the ability to fulfill the tasks listed in Article 39 of the GDPR	In the call for a DPO's appointment, a controller explicitly required that the candidates must have personal qualities, including integrity and high professional ethics. According to the EDPS for EUI's DPOs, the DPOs' ability to fulfill their tasks should be referred to their personal qualities and knowledge and their position within the organization.
Educational qualification	DPOs could have a variety of qualifications in law and computer science, security, and privacy	They cannot, however, be uniquely determined. An Italian court ruling asserts that holding an ISO 27001 certification cannot be a binding prerequisite in the selection procedure for a DPO's appointment.

internal ones may be information that a security operations center (SOC) or the IT staff provides to a DPO about events and incidents of security. The national computer security incident response team (CSIRT) is an external source that provides prealerts, alerts, bulletins, and information regarding risks and incidents. For instance, in case of a data breach, a DPO should collaborate with the internal IT department (if available) and later refer to the national CSIRT. As a further example, considering the interaction between a DPO and an SOC, the DPO will not have direct access to a security incident and event management system for an independent analysis of the inputs collected from the connected security devices and sensors.¹³ Instead, the DPO will refer to summary reports prepared by security analysts. In the case of uncovering a data breach, direct contact with security analysts could help obtain more information about the incident and better determine its impact and extent. Unfortunately, in many places (e.g., small public administrations), the “IT security department” is just one IT person who, among his or her other duties, knows little about security. The DPO may end up being the only security expert.

Currently available technology can help DPOs make it easier to carry out their tasks. For example, using requirement analysis tools in software development or procurement could improve compliance with the data-protection-by-design principle.

Additional support comes from research. Research findings can provide DPOs with insights into where to focus their efforts. According to this vision, the DPO advising task is “driven by research.” For example, Tang et al.¹⁴ find that users have difficulties understanding the technical terms used in privacy policies because they misunderstand and misconstrue them. As a result, privacy policies themselves are misunderstood and misinterpreted. Considering the results of this and other similar studies helps the DPO understand training gaps in the firm’s workforce.

The goal of compliance with the GDPR makes the DPO’s role dual. This data protection specialist is both the person who controls the processing activities in the organization and the person who acts as a wise

advisor to management. This tension could be problematic as the DPO needs information to carry out his or her duties. At the same time, the manager needs support in determining the purposes and means of processing personal data without giving the DPO too much information.

The duties assigned to the DPO role can quickly put this person in conflict with the organization for which he or she works. This case could happen, especially

in organizations with a negative attitude toward data protection. For example, Hadar et al.¹⁵ reported a qualitative study where 17 developers out of 27 declared that the climate of the organization they worked for was averse to data protection. Developers have reported that

Developers have reported that they must comply with organizational norms against data protection laws, contradictory to the company’s formally stated policies.

they must comply with organizational norms against data protection laws, contradictory to the company’s formally stated policies. In these circumstances, DPOs who carry out their duties will likely experience conflicts with management. Casutt and Ebert¹¹ found a similar outcome. They showed that DPOs experienced an inherent conflict between complying with the law and realizing the organization’s project whenever there is a gap between privacy requirements and those of the organization for which the DPO works.

A potential limitation of our research is that we based our scenarios on a detailed analysis of 90 specific cases, mostly of Italian origin, and court decisions may differ across EU member states. Several factors mitigate this issue. First, the relevant legislation (the GDPR) is a single regulation for all EU member states and is directly applicable to them, regardless of the national legislation, and the EDPB is tasked with facilitating the consistent application of data protection rules throughout the EU and promoting cooperation among the SAs of individual EU member states. Second, we reviewed supervisory decisions of several countries,¹ including more than 1,400 cases from <https://www.enforcement-tracker.com/>. So we are reasonably confident that our scenarios will stand the test of cross-border analysis.

Although we do not have an engineering solution for the DPO’s problems, at least being aware of the concrete problems is the first step toward a solution. ■

Acknowledgment

This work was supported in part by the EU under the H2020 Leadership in Enabling and Industrial

Technologies program under grant agreement 830929 (CyberSec4Europe). Francesco Ciclosi is the corresponding author. This article has supplementary downloadable material available at <https://arxiv.org/abs/2212.07712>, provided by the authors.

References

1. D. Korff and M. Georges. *The DPO Handbook Guidance for Data Protection Officers in the Public and Quasi-Public Sectors on How to Ensure Compliance with the European Union General Data Protection Regulation*. (2019). [Online]. Available: https://www.academia.edu/39968880/The_DPO_Handbook_Guidance_for_data_protection_officers_in_the_public_and_quasi_public_sectors_on_how_to_ensure_compliance_with_the_European_Union_General_Data_Protection_Regulation
2. R. K. Yin, *Case Study Research and Applications*. Newbury Park, CA, USA: Sage, 2018.
3. G. Almeida Teixeira, M. Mira da Silva, and R. Pereira, "The critical success factors of GDPR implementation: A systematic literature review," *Digit. Policy, Regulation Governance*, vol. 21, no. 4, pp. 402–418, 2019, doi: 10.1108/DPRG-01-2019-0007.
4. V. Diamantopoulou, A. Tsohou, and M. Karyda, "From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls," *Inf. Comput. Secur.*, vol. 28, no. 4, pp. 645–662, 2020, doi: 10.1108/ICS-01-2020-0004.
5. P. Ryan, M. Crane, and R. Brennan, "Design challenges for GDPR RegTech," in *Proc. 22nd Int. Conf. Enterprise Inf. Syst.*, SCITEPRESS - Science and Technology Publications, 2020, pp. 1–8, doi: 10.5220/0009464507870795.
6. A. Chatzipoulidis, T. Tsiakis, and T. Kargidis, "A readiness assessment tool for GDPR compliance certification," *Comput. Fraud Secur. Bull.*, vol. 2019, no. 8, pp. 14–19, 2019, doi: 10.1016/S1361-3723(19)30086-7.
7. Y.-S. Martin and A. Kung, "Methods and tools for GDPR compliance through privacy and data protection engineering," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, 2018, pp. 108–111, doi: 10.1109/EuroSPW.2018.00021.
8. M. Malatji, A. Marnewick, and S. von Solms, "Validation of a socio-technical management process for optimising cybersecurity practices," *Comput. Secur.*, vol. 95, p. 101,846, Aug. 2020, doi: 10.1016/j.cose.2020.101846.
9. R. Layton and S. Elaluf-Calderwood, "A social economic analysis of the impact of GDPR on security and privacy practices," in *Proc. 12th CMI Conf. Cybersecurity Privacy (CMI)*, 2019, pp. 1–6, doi: 10.1109/CMI48017.2019.8962288.
10. "Guidelines on Data Protection Officers ('DPOs') - WP243 Rev. 01," European Commission, Brussels, Belgium, 2017. [Online]. Available: <https://ec.europa.eu/newsroom/article29/items/612048>
11. N. Casutt and N. Ebert, "Data protection officers: Figureheads of privacy or merely decoration," in *Proc. 16th Eur. Conf. Manage., Leadership Governance*, Academic Conferences International, 2020, p. 39.
12. N. Dragoni, A. Lluch Lafuente, F. Massacci, and A. Schlichtkrull, "Are we preparing students to build security in? A survey of European cybersecurity in higher education programs [Education]," *IEEE Security Privacy*, vol. 19, no. 1, pp. 81–88, Jan./Feb. 2021, doi: 10.1109/MSEC.2020.3037446.
13. S. Bhatt, P. K. Manadhata, and L. Zomlot, "The operational role of security information and event management systems," *IEEE Security Privacy*, vol. 12, no. 5, pp. 35–41, Sep./Oct. 2014, doi: 10.1109/MSP.2014.103.
14. J. Tang, H. Shoemaker, A. Lerner, and E. Birrell, "Defining privacy: How users interpret technical terms in privacy policies," *Proc. Privacy Enhancing Technol.*, vol. 2021, no. 3, pp. 70–94, 2021, doi: 10.2478/popets-2021-0038.
15. I. Hadar et al., "Privacy by designers: Software developers' privacy mindset," *Empirical Softw. Eng.*, vol. 23, no. 1, pp. 259–289, 2018, doi: 10.1007/s10664-017-9517-1.
16. B. G. Glaser and J. Holton, "Remodeling grounded theory," *Forum Qualitative Sozialforschung/Forum, Qualitative Soc. Res.*, vol. 5, no. 2, May 2004, Art. no. 4. [Online]. Available: <https://www.qualitative-research.net/index.php/fqs/article/download/607/1316/>

Francesco Ciclosi is a Ph.D. student in information engineering and computer science at the University of Trento, Trento, 38123, Italy. He has been a data protection officer for an Italian city for the past five years and is currently on leave from the Ministry of Enterprises and Made in Italy, 00187 Rome, Italy. Previously, he was an adjunct professor of computer science for five years at the University of Macerata, 62100 Macerata, Italy. His research interests include methodologies for privacy in sociotechnical systems. Ciclosi received a master's degree in computer science security from the University of Milan "La Statale." Contact him at francesco.ciclosi@unitn.it.

Fabio Massacci is a professor at the University of Trento, Trento, 38123, Italy, and Vrije Universiteit, Amsterdam, 1081 HV, The Netherlands. He participates in the CyberSec4Europe pilot and leads the H2020 AssureMOSS project. Massacci received a Ph.D. in computing from the University of Rome "La Sapienza." For his work on security and trust in sociotechnical systems, he received the Ten Year Most Influential Paper Award at the 2015 IEEE International Requirements Engineering Conference. He is a Member of IEEE. Contact him at fabio.massacci@ieee.org.