info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

Ensuring the Availability of DPO Contact Details: A Comparison of the EU and UK GDPR

Introduction

The Bavarian Data Protection Authority (BayLDA), in its 2025 annual report, highlights an issue that may appear technical but is in fact a fundamental compliance requirement: a separate, dedicated communication channel must be provided for the Data Protection Officer (DPO). This is not merely an organizational recommendation, but an obligation directly derived from the GDPR—regulated with slightly different emphases, yet with identical substance, in both the EU and UK legal systems.

Relevant Provisions under the EU GDPR

Starting point: the obligation of confidentiality

Article 38(5) of the EU GDPR provides that the Data Protection Officer shall be bound by confidentiality or secrecy concerning the performance of their tasks.
This provision does not merely establish a behavioral expectation for the DPO, but also implies a structural requirement: the confidential nature of communications addressed to the DPO cannot be ensured if such communications are received through the controller's general communication channels that are accessible to a broader range of personnel within the organization.

The obligation to provide resources

Article 38(2) of the GDPR requires the controller to ensure that the Data Protection Officer is provided with adequate resources to carry out their tasks. The European Data Protection Board (EDPB), in its Guidelines 243/2017 on Data Protection Officers, clearly states that the provision of resources also extends to the infrastructural conditions necessary for communication with data subjects.[(2),(3)]

The obligation to publish contact details

Articles 13(1)(b) and 14(1)(b) of the GDPR require that the contact details of the Data Protection Officer be included in the privacy notice provided to data subjects. Article 37(7) further requires that the controller publish the DPO's contact details and communicate them to the supervisory authority.
It is important to emphasize that not only the existence, but also the quality of the published contact details is subject to regulation.

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

The BayLDA's 15th Activity Report (2025), section 5.1, explicitly states that using the same email address for both the controller and the DPO is unlawful, as it undermines the ability to comply with the obligation of confidentiality and prevents data subjects from establishing an independent and confidential line of communication.[1]

Relevant Provisions under the UK GDPR

Following its departure from the EU, the United Kingdom established its own data protection regime. While the text of the UK GDPR largely mirrors that of the EU GDPR, there are differences in interpretative emphasis and supervisory practice.

Structural Parallels with the EU GDPR

Article 38(5) of the UK GDPR reproduces verbatim the confidentiality obligation found in the EU GDPR. Articles 37(7) and 38(2) likewise include the requirements to publish contact details and to provide adequate resources.
These provisions are supplemented by the Data Protection Act 2018 (DPA 2018), which provides the statutory framework for the application of the UK GDPR.

The ICO's Interpretative Practice

The UK supervisory authority, the Information Commissioner's Office (ICO), confirms in its guidance on Data Protection Officers (ICO, *Guide to Data Protection: Data Protection Officers*, last updated 2023) that DPO contact details must be published both in privacy notices and in communications with the supervisory authority.
The ICO guidance emphasizes that data subjects must be able to contact the DPO directly and easily—this corresponds to the requirement of an independent communication channel in the UK context, although it is less explicitly articulated in statutory terms and is instead framed as good practice (ICO, *Guide to Data Protection: DPOs*, Chapter 2, "Contact details" subsection).[6]

Difference: Flexibility of the UK Approach

In general, the ICO's supervisory practice is less casuistic in this area than that of the BayLDA. ICO case law does not contain a decision addressing the separation of DPO communication channels with the same level of detail as section 5.1 of the BayLDA's 2025 report.
Nevertheless, the underlying expectations lead to the same conclusion: if the DPO's contact details do not allow for confidential communication, this results in a breach of both the confidentiality obligation and the requirement to provide adequate resources.

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

Comparison: Similarities and Differences

Criterion	EU GDPR	UK GDPR
Confidentiality Obligation	Article 38(5)	Article 38(5)
Resource Provision	Article 38(2)	Article 38(2)
Disclosure requirement	Article 37(7)	Article 37(7)
Dedicated channel	Mandatory BayLDA 2025	ICO Guidelines
Supervisory precedent	BayLDA 5.1. (2025)	There is no direct case law
Subject to sanctions	Article 83 of the GDPR	DPA 2018 + Article 83 of the UK GDPR

What does this mean in practice?

Section 5.1 of the BayLDA's 2025 Annual Report outlines concrete organizational requirements that can be regarded as best practice in both legal systems:

- At the email level: a dedicated functional address—such as *dsb@* or *dpo@*—to which only the Data Protection Officer, any deputy, or staff reporting directly to the DPO have access.
- At the postal level: within the controller's mailing system, an identifiable process ensuring that correspondence addressed to the DPO is forwarded unopened—for example, marked "For the attention of the Data Protection Officer."
- At the level of access rights: technical measures must ensure that neither IT administrators nor senior management have access to the DPO's mailbox without justification, unless there is a legal basis permitting such access.
- At the level of information provision: the privacy notices issued under Articles 13 and 14 must display this dedicated contact channel, rather than a general customer service contact.

For organizations operating in the EU, the BayLDA's 2025 report sends a clear message: supervisory authorities actively assess not only the existence, but also the quality of DPO contact details.
In a Bavarian or other EU Member State context, listing a general customer service email address as the DPO contact can in itself constitute an infringement. Although the BayLDA closed the examined cases without sanctions, a precedent has been established.
Under Article 83 GDPR, such structural deficiencies may be subject to fines of up to €10 million or up to 2% of the global annual turnover.
The situation for UK organizations is currently subject to less explicit supervisory pressure, as the ICO has not yet issued case law of comparable detail to that of the BayLDA on this specific

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

issue. However, the new complaint-handling obligations introduced by the DUAA—with a 30-day acknowledgment deadline and expectations regarding dedicated channels—create an indirect compliance requirement.
If an organization routes complaint handling through the DPO, the absence of a separate contact channel may simultaneously breach Article 38(5) UK GDPR and the new complaint-handling expectations.[4]

Organizations operating under dual jurisdiction face the most complex scenario.
Entities active in both the EU and the United Kingdom—for example, a London-based company serving EU customers—are effectively subject to two parallel compliance regimes.
In practice, this means that maintaining a single DPO contact point may not be sufficient: where EU and UK data subject groups are distinct, consideration must also be given to which contact details are valid in relation to which supervisory authority.
Under Article 27 GDPR and its UK equivalent, a representative may be required in both jurisdictions, and the DPO's contact details must be aligned accordingly.
In a poorly designed structure, both an EU supervisory authority (such as the BayLDA or another Member State authority) and the ICO may simultaneously identify the same deficiency, creating a risk of cumulative sanctions.

Summary

The regulation of DPO contact details may appear to be a technical detail, but in reality it represents the organizational manifestation of core GDPR principles—particularly transparency and accountability.
While the wording of the EU GDPR and UK GDPR is largely aligned on this issue, the BayLDA's supervisory practice provides more detailed and assertive guidance, whereas the ICO has so far articulated similar expectations in a less prescriptive manner.
Final conclusion: The correct compliance model is the same in both legal systems. It is not sufficient merely to publish the DPO's name and contact details; it must also be ensured that those contact details enable a genuinely confidential line of communication between the data subject and the DPO, without interference from the controller's organization.

Sources

1. BayLDA, *15th Activity Report 2025*, Section 5.1, p. 25 (*Provision of a separate contact option for Data Protection Officers*)
2. Regulation (EU) 2016/679 (GDPR): Article 13(1)(b), Article 14(1)(b), Article 37(7), Article 38(2), Article 38(5)
3. EDPB, *Guidelines on Data Protection Officers (DPOs)* (WP 243 rev.01)

info@educage.training
56 St. Williams Way, Norwich, England, NR7 0AP
+44 7916 768521; +43 681 207 85390

4. UK GDPR (as amended by the EU Exit Regulations): Article 37(7), Article 38(2), Article 38(5)
5. Data Protection Act 2018
6. ICO, Guide to Data Protection