

GDPR | ARTICLE 37 | EDPB

# Your company has not appointed a DPO. Are you sure you can justify that decision?

The question is not only whether a DPO exists. It is whether the decision can be defended.

When DPO appointment is mandatory

## Article 37 does not leave everything open

Designation is mandatory in three main scenarios: public authority or body, large-scale regular and systematic monitoring, and large-scale processing of special categories of data or criminal data.

**Common mistake**

**“We are an SME, therefore we do not need a DPO”**

That reasoning is insufficient and often legally weak. What matters is the organisation’s core activities, monitoring, processing scale and sensitivity of the data.

### Accountability

## **Not appointing a DPO may be legitimate. But the position must be defensible.**

The GDPR requires the organisation to demonstrate that it assessed its position correctly. EDPB guidance recommends documenting the analysis, especially where the answer is not obvious.

**Internal checklist**

## **If no DPO is appointed, what should be documented?**

Core activities, regular and systematic monitoring, scale of processing, type and sensitivity of data, reasoned conclusion, decision date and planned reassessment.

### Warning signs

## The decision may be wrong if...

The organisation relies on video surveillance, scoring, profiling, geolocation, health or biometric data at meaningful scale, or if an old decision has never been reviewed.

## Conclusion

# The real test is not “do we have a DPO?”

The real test is whether the organisation can defend the decision it made. Ahkoris helps assess DPO obligations and document a technically defensible position.