

### ARTICLE 28 CHECKLIST

Pursuant to Article 28, contracts between controllers and processors (and processors and subprocessors) must do the following:

REQUIREMENT	COMPLIANCE	CITATION
1. State the subject matter and duration of the processing	<input type="checkbox"/>	Art. 28(3)
2. State the nature and purpose of the processing	<input type="checkbox"/>	Art. 28(3)
3. State the types of personal data and categories of data subjects	<input type="checkbox"/>	Art. 28(3)
4. State the obligations and rights of the controller	<input type="checkbox"/>	Art. 28(3)
5. Require that processors process personal data only on documented instructions from the controller (unless required to do otherwise by law)	<input type="checkbox"/>	Art. 28(3)(a)
6. Require that processors transfer personal data internationally only on documented instructions from the controller (unless required to do otherwise by law)	<input type="checkbox"/>	Art. 28(3)(a)
7. Require that processors ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality	<input type="checkbox"/>	Art. 28(3)(b)
8. Require that processors take all measures required pursuant to Article 32 (Security of Processing), which includes the obligation to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk	<input type="checkbox"/>	Art. 28(3)(c)
9. Require that processors obtain authorization from the controller before engaging a subprocessor and provide notice to the controller of any intended changes concerning the addition or replacement of processors, thereby giving the controller the opportunity to object to such changes	<input type="checkbox"/>	Art. 28(3)(d)
10. Require the processor to contractually flow down the same data protection obligations in its contract with the controller to all subprocessors and hold the processor fully liable to the controller for the subprocessors' performance of such data protection obligations	<input type="checkbox"/>	Art. 28(3)(d)
11. Require that processors assist the controller by appropriate technical and organizational measures in responding to data subject rights requests	<input type="checkbox"/>	Art. 28(3)(e)

REQUIREMENT	COMPLIANCE	CITATION
12. Require that processors assist the controller in responding to a data breach (including but not limited to complying with breach notification obligations)	<input type="checkbox"/>	Art. 28(3)(f)
13. Require that processors assist the controller with data protection impact assessments and consultations with the supervisory authority, when required	<input type="checkbox"/>	Art. 28(3)(f)
14. Require that processors delete or return all personal data to the controller, at the choice of the controller, after the end of the provision of services relating to the processing (unless continued storage is required by law)	<input type="checkbox"/>	Art. 28(3)(g)
15. Require that processors make available to the controller all information necessary to demonstrate their compliance with their Article 28 obligations and allow for and contribute to audits conducted by or at the request of the controller	<input type="checkbox"/>	Art. 28(3)(h)