Checklist 3: What is required in a processing agreement?

Controllers can have another entity process personal data on their behalf. Outsourced processing thus concerns personal data produced and processed by the contract, not data of the contractor or its staff.

Processing by a processor requires a **contract or other legal act** under Union or Member State law, which is **binding on the processor** and sets out:

- purpose, duration, nature & scope of processing
- categories of data & data subjects
- retention period
- data location & data access (based on preliminary risk assessment may be limited or not to EEA)
- recipients of data and data transfers (within the EUI, to other EUIs, to third countries or international organisations)
- security measures (guaranteeing at minimum the same level of security for the personal data as the controller)
- prohibition of disclosure of data – reference to the Protocol on Privileges and Immunities of the EU
- any additional data protection laws (e.g. ePrivacy Directive, NIS Directive) – if applicable
- processor may only act upon documented instructions of controller, unless required to do so by Union or Member State law (instructions also on transfers of personal data and assistance to controller)
- sub-contracting only with prior written authorisation of controller, information in due time before any changes
- confidentiality measures, access only on a need to know basis to authorised persons
- auditing rights by controller of processors and sub-processors
- cooperation, on request, with the EDPS in the performance of his or her tasks (including EDPS' audit / investigation of processors and sub-processors)
- division of tasks between joint controllers – if applicable – so that processor knows how to assist which joint controller
- assistance with data subject rights requests
- assistance with controller obligations (security and data breach notification, data protection impact assessment and prior consultation, confidentiality of electronic communications, information and consultation of EDPS) and record of processing on behalf of controller
- assistance with data breaches – set specific deadline
- choice by controller for processor to return or delete the data at the end of the processing
- obligation to inform the controller if its instruction infringes Regulation 2018/1725 or other Union or Member State data protection provisions
- ground for termination in case of substantial non-compliance of processor, liability etc.
- applicable data protection law (Regulation 2018/1725)
- other applicable provisions affecting data protection, e.g. choice of applicable law and jurisdiction (Member State of EUI's seat), amendments (only bilateral) etc.

The contract or other legal act may be based, in whole or in part, on **standard contractual clauses for processors adopted by the EDPS or the EC**.