CHECKLIST - APPOINTING A DATA PROSESSOR

For organisations using a third-party/supplier to process data on their behalf)

1. BEFORE APPOINTING THE PROCESSOR

- [ ] Confirm your organisation is the “Controller” and will remain responsible for personal data processing.
- [ ] Ensure the potential processor’s role and activities are clearly understood (i.e., they will act only on your instructions).
- [ ] Identify the categories of personal data to be processed (types of data, types of data subjects).
- [ ] Define the purpose, nature, subject-matter and duration of the processing arrangement.
- [ ] Check the processor’s technical and organisational security measures for the data.
- [ ] Ask about sub-processors: whether the processor will engage any, and if so under what terms.
- [ ] Evaluate whether the processor can assist you in fulfilling data subject rights (access, rectification, erasure, etc.).
- [ ] Plan how you will review the processor’s compliance (audits, inspections, documentation).

2. CONTRACT/LEGAL AGREEMENT

Prepare a written contract (or other legal act) with the processor which sets out clearly:

- [ ] The subject-matter & duration of processing;
- [ ] The nature & purpose of processing;
- [ ] The type of personal data and categories of data subjects;
- [ ] The obligations and rights of the controller.

Include that the processor:

- [ ] Will process only on documented instructions from the controller;
- [ ] Ensures authorised persons processing the data are under confidentiality obligations;
- [ ] Implements appropriate technical & organisational measures for security;
- [ ] Respects conditions for any sub-processor use;
- [ ] At the controller’s choice, returns or deletes personal data after the service ends (unless law requires retention).
- [ ] Makes available information to demonstrate compliance and allows audits/inspections.

3. ONGOING MONITORING & OBLIGATIONS

- [ ] Monitor that the processor continues to act only on your instructions and follow the contract.
- [ ] Check regularly that the processor's security measures remain appropriate given the nature of the processing.
- [ ] Ensure the processor supports you in meeting your obligations under the relevant data protection law (for example: your duties to respond to data subject rights, to review high-risk processing, to notify personal data breaches).
- [ ] If any sub-processors are engaged, ensure you (as controller) have oversight and that they're subject to equivalent obligations.
- [ ] At the end of the processing service: verify that the processor returns or securely deletes the data (depending on instructions) and that no residual copies remain unless required by law.
- [ ] Keep records/documentation showing how the appointment and monitoring of the processor has been managed, in order to demonstrate compliance.

4. RISK & COMPLIANCE ASSESSMENT

- [ ] Consider whether the processing by the processor is "high risk" (e.g., large volumes, special category data, systematic monitoring) and whether additional safeguards are needed.
- [ ] Ensure you have considered the legal basis, transparency obligations and data subject rights in your ongoing relationship with the processor.
- [ ] Update your register of processing activities (or equivalent) to reflect the processor relationship.
- [ ] Review and update the contract and arrangements periodically (e.g., when scope changes, technology changes, additional sub-processors involved).