Data protection checklist

Until all five have answers, the tool is not used with matter or client data.

1. Who is the processor, and under which agreement?

- [ ] The agreement is signed by the company, not by an employee
- [ ] You know which legal entity is your counterparty and which plan it covers
- [ ] Your notes say what the agreement covers and what it does not

2. What is the basis for the transfer to a third country, and has it been assessed?

- [ ] You know which transfer mechanism applies
- [ ] The assessment is done, dated and read by the data protection officer
- [ ] It ends in a list of matter types that are not entered
- [ ] There is a plan for what happens if the adequacy decision falls

3. How long is data kept, and who can see it?

- [ ] You know the default and which settings your plan offers
- [ ] Retention periods are set per matter type
- [ ] Permissions in connected systems have been reviewed

4. What happens if an authority requests the data?

- [ ] One of three is documented: the vendor has undertaken to inform and object, the risk is accepted for named matter types, or those matters are kept out

5. Which matters are kept out of the tool?

- [ ] The list exists, by matter type, and has an owner
- [ ] Everyone in the department knows it
- [ ] It is reviewed each time the assessment is reviewed

You should now hold:

- [ ] The processor agreement with notes
- [ ] The transfer assessment
- [ ] Any impact assessment
- [ ] The settings list
- [ ] The policy with the list of matters kept out
- [ ] The training material