Checklist
Data Processing Agreement

de groote de man

A DPA must contain a description of the following details:

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

A DPA must include the following mandatory obligations:

- [ ] The processor must only act on the written instructions of the controller (unless required by law to act without such instructions).
- [ ] The processor must ensure that the personnel used by the processor for processing the data are subject to a duty of confidence.
- [ ] The processor must take appropriate measures to ensure the security of processing.
- [ ] The processor can only engage a sub-processor with the prior consent of the data controller and a written contract and must ensure it flows down these obligations to any sub-processor. The processor remains responsible for any processing of the sub-processor.
- [ ] The processor must assist the data controller to comply with requests from data subjects exercising their right to access, rectify, erase, or object to the processing.
- [ ] The processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and to conduct data protection impact assessments.
- [ ] The processor must delete or return all personal data to the controller as requested at the end of the contract.
- [ ] The processor must demonstrate its compliance with these obligations and submit to audits and inspections by the controller (or by a third party mandated by the controller).
- [ ] The processor must provide the controller with whatever information it needs to ensure that they are both meeting their obligations under the GDPR, and must inform the controller when, in its opinion, the controller's instruction would breach Union or Member State law.
- [ ] Nothing within the contract relieves the processor of its own direct responsibilities under the GDPR (not mandatory, but recommended).

In addition, a checklist of a processor's direct responsibilities:

- [ ] A data processor can only act on the written instructions of the controller.
- [ ] A data processor can not use a sub-processor without the prior written authorisation of the controller.
- [ ] A data processor must co-operate with supervisory authorities.
- [ ] A data processor must ensure the security of its processing in accordance with the requirement to take appropriate technical and organisational measures.
- [ ] A data processor must keep records of its processing activities (unless exempt).
- [ ] A data processor must notify the controllor about any personal data breaches in accordance with the rules on personal data breach notification.
- [ ] A data processor must appoint a data protection officer (if required).
- [ ] A data processor must appoint (in writing) a representative within the EU/EEA if required by the GDPR.

More information regarding DPA, privacy or GDPR?

Ask our Privacy & IT experts at

WWW.DEGROOTE-DEMAN.BE