

## **Annex 1 – The contracting authority’s specification of requirements**

The Danish Competition and Consumer Authority (DCCA) is to review the primary software for design and conducting computer-based behavioural experiments.

The software will be used for conducting studies about consumer behaviour and market simulations through randomized controlled experiments (online and lab based).

### **The software must live up to the following minimum requirements:**

- It must be possible to randomize participants/respondents into different versions of a study, with the option of equal distribution.
- It must be possible to present audio, video and image to be shown as stimuli to participants/respondents.
- It must be possible to randomize the order of stimuli shown and show stimuli randomly drawn from a subset of stimuli.
- It must be possible to distribute studies via external panels (e.g. via individual unique links to the study).
- It must be possible to customize elements in a study, such as the appearance and functionality of a study (e.g. through custom coding).
- It must be possible to add survey elements to a study.
- It must be possible to download study data in csv files or excel file-format.

### **GDPR Compliance:**

The supplier shall be compliant with Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) when it processes personal data in relation to the provision of the services.

The supplier shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk related to the processing of personal data, cf. GDPR art. 32, section 1. Moreover, the supplier must store personal data in the EU/EEA. Transfers of personal data to countries outside the EU/EEA is not permitted unless the supplier has implemented technical measures ensuring that the supplier or third parties, including authorities, in the country of destination cannot access the data “in the clear”, e.g. by encrypting the data and storing the decryption key separate at an EU/EEA based supplier that is solely under the jurisdiction of the European Union Member States and Member State law so only that EU/EEA based party (e.g. the Danish Competition and Consumer Authority) can read/decrypt data.

### **Duration of the contract:**

The contract is valid for four years.

