RED C Data Protection Policy

Date created: 21/05/2005

Last revised: 29/06/2017

RED C shall at all times comply with the Data Protection Act 1988 and 2003 (as applicable) (the "Legislation") and any regulations made under or separate to the Legislation or any other legislation relating to the protection of personal data.

As Data Processors our responsibility as a market research agency is to ensure that customer information is stored and handled in a safe and secure manner at all times. When using client lists RED C act as Data Processors.

Customer lists are only used for the intended purpose of the client – the market research project. All customer lists are password protected on the internal server. Soft copies are only saved on the server – never on desktops or USB keys. If printed, they are stored in a locked filing cabinet when not in use and are disposed of using confidential waste bins. All customer lists are securely deleted from the server within a timeframe agreed with the client.

In the absence of any express instructions to the contrary, all personal data received by RED C from any client shall be retained for as long as is necessary, having consideration to the processing that was carried out, and in any event for no longer than 6 months once such processing ceases and thereafter such data shall be securely deleted and/or destroyed thereafter, whether in electronic or manual format.

Where it is necessary to transfer personal data from one location to another, whether physically or electronically, the necessary information security precautions need to be taken. This includes the use of electronic encryption technology.

The RED C server has adequate security provided by Provident Technology who have signed an NDA. Our server can be accessed by all RED C staff who have signed a Confidentiality Agreement and abide the Market Research Society Code of Conduct. We have procedures in place to control access to the computer room where the server is held. The server is in a locked cabinet to protect against access, spillage and other potential hazards and is raised to avoid flood threat.

The area is temperature-controlled by air-conditioning and fire-doors are part of the make-up of the building. Back-ups are conducted at our Dublin and Dundalk offices every evening. Back-up data is stored in a fire-proof safe off-sire. We are in a hospital area so outages due to electricity supply problems are minimal.

RED C will refrain from disclosing personal data to any third parties other than to permitted sub-contractors to whom disclosure is reasonably necessary in order for the us to carry out the Services, provided that in all cases:

a. such disclosure is made subject to written terms substantially the same as the terms contained in this processor agreement;

b. such disclosure has been approved in writing in advance by the client; and

c. upon the request of the client, promptly provide a written description of the technical and organisational measures employed by it and/or any of its permitted sub-contractors, detailed to such a level that the client can determine whether or not, in connection with personal data, the Supplier and its permitted sub-contractors are complying with their obligations under this Agreement. If, in the clients opinion, the measures employed by the Supplier and/or its permitted sub-contractors are not sufficient to ensure compliance with their obligations under this Agreement, the Supplier shall take all steps (or procure that its permitted sub-contractors take all steps) which are reasonably required to ensure that such compliance is achieved;

d. afford to the client (and procure that its permitted sub-contractors afford to the client) access on reasonable notice and at reasonable intervals to any premises where the relevant personal data are being processed to enable The client to ensure that the Supplier is complying with its obligations under this Agreement and/or that the Supplier's permitted sub-contractors are complying with the equivalent contractual obligations imposed on them;

e. promptly refer to The client any requests, notices or other communication from data subjects, the office of the Data Protection Commissioner or any other law enforcement agency relating to personal data for The client to resolve;

f. at no additional cost, provide such information to The client as The client may reasonably require, and within the timescales reasonably specified by The client, to allow The client to comply with rights of data subjects, including subject access, or with notices served by the office of the Data Protection Commissioner; and

Our Data Protection Officer – Janna Howard (a RED C employee) - ensures adherence to secure storage and handling of data by all RED C employees.

How to contact us

Questions regarding this policy, complaints about our practices and access requests should be directed to the RED C Research Data Protection Officer via e-mail at info@redcresearch.ie or by mail to Ground Floor, Block G, Eastpoint Business Park, Clontarf, Dublin 3, Ireland.