

CORE|DATA

CONFIDENTIALITY + DATA SECURITY POLICY

CoreData 2017

Contents

Privacy Policy Overview.....	3
Collection of personal information	3
Informed consent.....	4
Storage and security of personal information	5
The use of data and personal information.....	6
Provision of personal information to third parties and cross border disclosure	7
Anonymity	7
Correction of personal information	8
Contacting us.....	8
CoreData.....	9
About Us.....	9

Privacy Policy Overview

CoreData strictly adheres to the AMSRS Code of professional behaviour in relation to research confidentiality and data security. This means that all responses are strictly confidential. Reports will only display highly aggregated data and will not allow identification of individual respondents. Only CoreData as the independent primary researchers will have access to raw unidentified data. CoreData shall never allow personal data they collect in a market research project to be used for any purpose other than market research. That means details will never be used for direct marketing.

CoreData maintains the highest standards of data security requiring careful management of data security and storage on protected servers. We have an exemplary track record of ensuring our clients data security since our inception over a decade ago. This is obviously a key requirement for our business viability and something we take very seriously.

Collection of personal information

Under the Privacy Act and Privacy Amendment (Enhancing Privacy Protection) Act 2012, personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable whether the information or opinion is true or not, and whether the information or opinion recorded in material form or not. All personal information that we collect, is reasonably necessary for the purposes relating to providing professional services to our clients or in conjunction with research into wider industry issues.

The types of personal information we collect includes, but is not limited to, contact details such as name, email, phone and mailing address and position/title. Where we provide services to a client, we may collect sensitive information in the performance of our services. In these circumstances, we rely on the client having informed you of this use and obtaining your consent.

If it is reasonable and practical to do so, we will collect personal information directly from you. This will include contact details and other information relevant to providing services to our client.

We may also collect personal information from third parties including but not limited to publically available sources. In these situations, we will take reasonable steps to ensure you are made aware that we hold your personal information and the matters listed above, unless an exemption applies under the Privacy Act.

In relation to our professional engagements, prior to commencing, we require clients to authorise the release, collection and retrieval of personal information to us. In addition, we require a client to provide us with confirmation that it has made, or will make those persons to whom the personal information relates, aware that we have their personal information, the reasons for its collection by us and that it may be further disclosed to governments or other

bodies (where necessary) for the purposes of completing the engagement. These authorisations and statements form part of our standard terms and conditions of engagement with clients.

We will not collect personal information unless the information is reasonably necessary for or directly related to one, or more of our functions or activities. If we are unable to collect personal information we reasonably require, we may not be able to do business with you or the organisation with which you are connected.

If we receive personal information about you that we did not ask for, or from someone other than you, and we determine that we could have collected this information from you had we asked for it, we will take reasonable steps to ensure that you are notified, as soon as practicable, that we have collected your personal information. If we could not have collected this personal information, we will lawfully de-identify or destroy that personal information.

In carrying out an engagement, it may be necessary for CoreData to obtain from a client personal and sensitive information about the employees of the client or other persons connected with the client's business. We will take reasonable steps to ensure that the individual's consent has been obtained by the client before collecting the sensitive information.

All data, including personal information is received on a confidential basis and CoreData has appropriate internal arrangements with its systems and staff to ensure that the confidentiality of the personal information is protected.

When you visit our web site, we (or our service providers) may obtain information from your personal computer that provides your internet address, your domain name (if applicable), and the previous sites you have visited and when you visited the web site.

When you visit the web site, our server may attach a 'cookie' to your computer's memory. This is done to help us store information on how visitors to our web site use it and the pages that may be of most interest. However, this information is not linked to any information you may provide and cannot be used to identify you and is therefore not personal information.

Informed consent

All research participants agree that they are providing informed consent to participate in the research by proceeding to complete the survey. This means that they have been informed about:

- The purpose of the research (included in the email invitation and landing page – further detail provided directly by CoreData if required with contact details included)
- Incentives for participation (Included in the terms and conditions link)
- Their right to decline to participate and to withdraw from the research once participation has begun
- The extent, if any, to which confidentiality of records identifying the respondent will be maintained and the limits of confidentiality
- An explanation of whom to contact for answers to pertinent questions about the research and research respondents' rights

Storage and security of personal information

CoreData strictly adheres to the AMSRS Code of professional behaviour in relation to research confidentiality and data security. This means that all responses are strictly confidential. Reports will only display highly aggregated data and will not allow identification of individual respondents. Only CoreData as the independent primary researchers will have access to raw unidentified data. CoreData shall never allow personal data they collect in a market research project to be used for any purpose other than market research, unless required by law. That means details will never be used for direct marketing.

CoreData maintains the highest standards of data security requiring careful management of data security and storage on protected servers. We have an exemplary track record of ensuring our clients data security since our inception over a decade ago. This is obviously a key requirement for our business viability and something we take very seriously.

CoreData conforms to current professional best practice relating to the keeping of records securely for an appropriate period of time after the project has ended. This includes password protection for access to its information technology systems and securing access to physical records.

The proposed period of time for which the Researcher should keep research records will vary with the nature of the information (e.g. whether they are identified or de-identified), the nature of the project (e.g. ad hoc, panel, repetitive) and the possible requirements for follow-up research or further analysis. Researchers may retain information in an identified form only while the details of the identity of the Respondent continue to be necessary for research purposes. Records should be kept in a manner in which it should be possible to reconstruct all the information originally collected with the exception of any personal identifiers.

All data is stored on secure servers with well-maintained firewall facilities. All data is additionally backed up daily to a secure offsite server that also has well-maintained firewall facilities. Security of our servers is managed by a dedicated IT provider who has explicitly agreed to adhere to the AMSRS standards for data storage and security.

Staffs that handle personal information have the knowledge, skills, training and commitment to protect it from unauthorized access or misuse. In the event that third parties are permitted under informed consent to access data, they must commit to the aforementioned privacy principles in a written contract.

The use of data and personal information

All research data, findings (except in the case of syndicated projects), research briefs and other information provided must not be disclosed to third parties without prior explicit arrangement, unless required by law. The transfer of information about Respondents is permissible between a Researcher and the Client where the intent of this is to limit research contacts by means of maintaining records about participation. This should not be done where this practice would allow personalised information to be extrapolated or where any research data gathered about an individual may be appended or inferred by the transfer.

Generally, we will use personal information only for the purposes for which it was collected.

The personal information collected by us may be used to:

- provide clients and other parties with our services or with other information requested;
- manage our relationship with you; and
- Notify you about our services or promotions.

We may use personal information about you for the primary purpose of providing you with our services, and other purposes you would reasonably expect us to use that information for, including sending you information about new developments, products, services, events, seminars and conferences by post, telephone or any form of electronic communication. We may use any email address or other personal information you provide to us at any time for this purpose.

At any time, you can opt out of receiving marketing material by contacting us by the means set out in the communication. You agree and acknowledge that even if you opt out of receiving marketing material, we will still send you essential information that we are required to send you relating to the services we provide.

Provision of personal information to third parties and cross border disclosure

Unless we are required to disclose your personal information by law, Court or arbitration proceedings, by a regulatory authority, under regulations (including those made under the Corporations Act) or to fulfil a professional duty, your personal information will only be used by or disclosed to persons working at or for CoreData and our contracted service providers. We will only disclose your personal information to third parties, without your consent, if permitted by the Privacy Act or authorised by some other law.

It may be necessary for us to transfer personal information we hold about you to an organisation outside Australia. We will transfer information outside Australia in a manner that is consistent with the requirements of the Privacy Act. By providing your personal information to us directly or via one of our clients you consent to this disclosure.

Anonymity

Respondent's anonymity must be strictly preserved. The respondents must give informed consent for data to be passed on in a form that allows them to be personally identified. The Researcher must ensure that the information will not be used for any non-research purposes and that the specified recipient of the information has agreed to conform to confidentiality requirements. The Client has no right to access the names and addresses of respondents unless express permission for this is received or if this is only to be used for managing project implementation and cannot be linked to actual responses.

All indications of the identity of Respondents must be permanently removed from the records of information they have provided as soon as they are no longer necessary for research purposes. Where it is necessary to retain identifying details, they must be stored securely and separately from other information the Respondent has provided (e.g. with the linkage maintained by the use of an intervening variable). Access to such material must be restricted to authorised research personnel within the Researcher's own organisation for specific research purposes (e.g. field administration, data processing, panel or "longitudinal" studies, or other forms of research involving recall interviews).

To preserve Respondents' anonymity not only their names and addresses but also any other information provided by or about them that could identify them (e.g. their Company and job title) must be safeguarded.

These anonymity requirements may be somewhat relaxed where the Respondent has given explicit permission for this under the conditions of 'informed consent'. This can be required where disclosure of names to a third is essential for research purpose such as data processing or further interview (e.g. an independent fieldwork quality check) or for further follow-up research. The original Researcher is responsible for ensuring that any such third party agrees to observe the requirements of this Code – in writing, if the third party has not

already formally subscribed to the Code. These anonymity requirements relate to any records from which the identity of the Respondent is apparent, or can reasonably be ascertained, including a Respondent's photograph, verbatim quotes and audio or videotaped interviews. Permission to observe an interview/group discussion by a third party must be gained from the respondent.

Please note that participation is voluntary, refusal to participate will involve no penalty or loss of benefits to which the respondent is otherwise entitled and the respondent may discontinue participation at any time without penalty or loss of benefits to which the respondent is otherwise entitled. All research respondents have the right to decline to participate and to withdraw from the research at any stage they desire.

When contacting us, you have the option to either not identify yourself or to use a pseudonym when you contact us, unless it is impracticable for us to communicate with you in that manner or unless we are required or authorised under Australian law, or a court or tribunal order, to deal with individuals who have identified themselves.

We take all reasonable steps to de-identify personal information in reports and work generally. The retention of personal information is subject to the same retention policy as other information in our possession, that is, material is generally destroyed ten years after its creation unless it is still required for legal reasons or is being retained as an historical record.

Correction of personal information

Under the Privacy Act, you have a right to seek access to your personal information, subject to any exemptions allowed under the Privacy Act.

If you request access to your personal information, you will need to prove your identity. We may also need to inform our client about your request under our contractual arrangements with them.

You also have the right to ask us to correct information about you to ensure the personal information we hold is accurate, up-to-date, complete, relevant and not misleading. Our policy is to consider any requests for access or correction in a timely way.

Contacting us

If you have any questions about this Privacy Policy, if you wish to complain about how we have handled personal information about you or if you wish to access or correct your personal information, please contact Tai Rotem, Director of Research at CoreData, on:

- Email: Tai.rotem@coredata.com.au
- Phone: 9376 9608

CoreData

About Us

CoreData Research is a global specialist financial services research and strategy consultancy. CoreData Research understands the boundaries of research are limitless and with a thirst for new research capabilities and driven by client demand; the group has expanded over the past few years into the Americas, Africa, Asia, and Europe.

CoreData Group has operations in Australia, the United Kingdom, the United States of America, Brazil, Singapore, South Africa and the Philippines. The group's expansion means CoreData Research has the capabilities and expertise to conduct syndicated and bespoke research projects on six different continents, while still maintaining the high level of technical insight and professionalism our repeat clients demand.

With a primary focus on financial services CoreData Research provides clients with both bespoke and syndicated research services through a variety of data collection strategies and methodologies, along with consulting and research database hosting and outsourcing services.

CoreData Research provides both business-to-business and business to- consumer research, while the group's offering includes market intelligence, guidance on strategic positioning, methods for developing new business, advice on operational marketing and other consulting services.

The team is a complimentary blend of experienced financial services, research, marketing and media professionals, who together combine their years of industry experience with primary research to bring perspective to existing market conditions and evolving trends.

CoreData Research has developed a number of syndicated benchmark proprietary indexes across a broad range of business areas within the financial services industry.

- Experts in financial services research
- Deep understanding of industry issues and business trends
- In-house proprietary industry benchmark data
- Industry leading research methodologies
- Rolling benchmarks

The team understands the demand and service aspects of the financial services market. It is continuously in the market through a mixture of constant researching, polling and mystery shopping and provides in-depth research at low cost and rapid execution. The group builds a picture of a client's market from hard data which allows them to make efficient decisions which will have the biggest impact for the least spend.



HEADQUARTERS

AUSTRALIA

CoreData Pty Limited
Suite 7, Level 9, 66 Hunter St
Sydney, NSW, 2000

T: +61 2 9376 9600

E: coredata@coredata.com.au

PHILIPPINES

CoreData Research Services Inc.
Unit E-1608 Philippine Stock Exchange
Centre,
Exchange Rd, Ortigas, Pasig City, 1605

T: +63 2 667 3996

E: info_ph@coredataresearch.com

UK

CoreData Research Ltd
6 Foster Lane,
London ECV 6HH
United Kingdom

T: +44 (0)207 600 5555

E: info_uk@coredataresearch.com

US

CoreData Research LLC
15 Court Square, #450
Boston, 02108

T: +1 (857)239 8398

E: info_us@coredataresearch.com