

Data Protection Policy

(approved for sharing with third-party business partners on the condition of confidentiality)

Version: 1.0

CONFIDENTIAL

This document has been created by Crosby Associates Media Limited. Its contents may be changed without prior notice. External web links are provided for information only. Crosby Associates Media Limited is not responsible for access to and correctness of the referenced content.

COPYRIGHT

The information contained in this document is intended only for the person or entity to which it is addressed and contains confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact Crosby Associates Media Limited and delete the material from any computer.

Copyright © 2018 Crosby Associates Media Limited. All rights reserved.

CONTACT INFORMATION

For questions relating to this document please contact:

Laura Bates

laura.bates@crosbyassociates.co.uk

CONFIDENTIAL

Contents

1 Introduction 3

 1.1 Audience..... 3

 1.2 Revision History..... 3

 1.3 Definitions 3

2 Background..... 4

 2.1 Introduction 4

 2.2 What is data protection law? 5

 2.3 How does the data protection law affect Crosby Associates Media Limited?..... 5

 2.4 What are we doing about it? 5

 2.5 The Data Protection Officer 5

 2.6 What are the consequences if we get it wrong?..... 6

 2.7 Why is the Policy important to Crosby Associates Media Limited?..... 6

 2.8 Want more information? 6

3 The Data Protection Policy 6

 3.1 Breakdown of the Rules 6

 3.2 Complying with the Rules 10

 3.3 Training on the Rules 10

 3.4 Responsibilities..... 10

1 Introduction

1.1 Audience

This document is an operational policy intended for Crosby Associates Media Limited staff. This policy covers all individuals working for Crosby Associates Media Limited at all levels and grades, including directors, employees, contractors, trainees, secondees, home-workers, part-time and fixed-term employees, and agency staff (collectively known as “Staff” in this policy and associated policies), and also third parties such as IT support companies who have access to Crosby Associates Media Limited's systems and information under contract.

This version of this document has been approved for disclosure to third parties that are business partners of Crosby Associates Media Limited in order to demonstrate Crosby Associates Media Limited's compliance with privacy and data security requirements. Business partners are asked to handle this document and its content as ‘commercial in confidence’.

1.2 Revision History

This document is reviewed every April and updated to reflect the modifications made to this document. With each revision a new entry is added to the table below, including the date of and the reason for the version change.

1.3 Definitions

Applicable Privacy Law(s): means the relevant data protection and privacy law(s) to which

Crosby Associates Media Limited is subject.

Data Controller: shall have the meaning described in the Data Protection Act 1998.

Data Processor: shall have the meaning described in the Data Protection Act 1998.

Customers: are prospective and current Customers of Crosby Associates Media Limited who require Crosby Associates Media Limited to process Personal Information on their behalf and subject to their instructions. For avoidance of doubt, Customers are Data Controllers in respect of such Personal Information.

Disclosure: refers to the release of, transfer of, provision of, access to, or divulging of Personal Information outside of Crosby Associates Media Limited.

Crosby Associates Media Limited employees: all Individuals working for Crosby Associates Media Limited at all levels and grades, including directors, trainees, secondees, home-workers, part-time and fixed-term employees, contractors, temporary or staffing agency personnel, and other outside personnel.

Individuals, People: refers to applicants, Crosby Associates Media Limited employees and contractors, former, present, and potential Staff, Customers of Crosby Associates Media Limited including but not limited to external Customers, and other external parties such as vendors or distributors.

Opt-in: Opt-in consent collection is an information collection and use mechanism in which Personal Information may not be collected, used, retained, or disclosed by the entity without the explicit consent of the individual.

Opt-out: Opt-out consent collection is a consent collection in which the individual's lack of action implies that a choice has been made regarding the individual's consent to Personal Information collection, use, retention, or Disclosure (e.g., unless an individual checks a box, his or her Personal Information may be shared with third parties for certain purposes).

Personal Information: any information that, alone or in combination with other information, identifies, relates to an identified or identifiable individual. Personal Information may pertain to Crosby Associates Media Limited employees, contractors, Customers, suppliers, business partners, or others. Personal Information includes "personal data" as defined in the Data Protection Act 1998.

Processing: refers to any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as collection; recording; organization; storage; adaptation or alteration; retrieval; consultation; use; Disclosure by transmission, dissemination or otherwise making available; alignment or combination; blocking; erasure or destruction.

Sensitive Personal Information: Personal Information that may require special consideration or protection due to the sensitive nature of the information. This includes, but is not limited to information about race, ethnicity, sexual life, philosophical opinions, religion, political opinions, union membership, actual or alleged criminal offences, and health-related data. This also includes any other covered information considered to be sensitive under local law. Depending on the jurisdiction, it may also be referred to as sensitive personal data.

Third Party: Third parties are Individuals or organizations excluding Crosby Associates Media Limited employees. Examples of third parties include, but are not limited to, contractors, Customers, vendors, distributors, suppliers, and applicable government agencies including regulatory agencies or law enforcement.

2 Background

2.1 Introduction

This is a statement of the data protection policy adopted by Crosby Associates Media Limited (the "Policy").

Crosby Associates Media Limited needs to collect and use certain types of information about People with whom it deals in order to operate effectively. These include current, past and prospective Crosby Associates Media Limited employees, suppliers, clients/Customers, and

others with whom it communicates. In addition, it may be a legal requirement to collect and use certain types of information, for example to comply with the requirements of government and regulatory bodies, for provision of business data. This Personal Information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer or recorded on other material – and there are safeguards to ensure such Personal Information is processed in line with in the Data Protection Act 1998.

This Policy sets out provisions relevant to all Crosby Associates Media Limited employees. Everyone in Crosby Associates Media Limited is accountable for upholding the requirements of this Policy. Failure to observe this Policy is a cause for disciplinary action which could involve dismissal.

All Crosby Associates Media Limited employees, temporary staff and contractors, as part of their induction to Crosby Associates Media Limited, must sign a copy of this Policy to confirm that they have read and understood this Policy and attend a Policy training session. This Policy covers the use of Personal Information about Crosby Associates Media Limited employees, temporary staff, contractors, Customers and prospective Customers, suppliers, clients and contacts.

This Policy is to be read in conjunction with the Information Security Policy and related internal policies and procedures.

We need to comply with the rules set out in this Policy about how we use Personal Information. No one is exempt from compliance with these rules.

2.2 What is data protection law?

Data protection law gives People the right to control how their Personal Information is collected and used.

2.3 How does the data protection law affect Crosby Associates Media Limited?

The use of Personal Information is critical to Crosby Associates Media Limited in order to:

- provide services to Customers;
- promote its goods and services;
- maintain its accounts and records; and
- support and manage its staff.

These activities, from start to finish, involve the use of Personal Information which will be covered by the Applicable Privacy Law.

Crosby Associates Media Limited provides services to Customers which involve the Processing of Personal Information. It is critical that our Customers are confident that their Personal Information is safe and that Crosby Associates Media Limited will use it in accordance with the Applicable Privacy Law.

We also need to ensure that the information we hold on our Crosby Associates Media Limited employees, temporary staff and contractors is used in accordance with the Applicable Privacy Law.

2.4 What are we doing about it?

Crosby Associates Media Limited treats compliance with their obligations seriously. We wish to obtain the highest possible standards to ensure that our internal procedures comply. We have developed this Policy to ensure that the Personal Information we collect and use is dealt with in accordance with the Applicable Privacy Law.

2.5 The Data Protection Officer

The role of the Data Protection Officer is to ensure that Crosby Associates Media Limited is, and remains, compliant with the requirements of the Applicable Privacy Law.

2.6 What are the consequences if we get it wrong?

Getting it wrong is serious for our business and our Customers. It could also lead to complaints from Individuals, compensation claims, fines from regulators, bad publicity for Crosby Associates Media Limited and personal liability for Crosby Associates Media Limited employees. Furthermore, if you deliberately fail to observe the Policy, we will consider disciplinary action against you.

2.7 Why is the Policy important to Crosby Associates Media Limited?

It is vital that those working in Crosby Associates Media Limited observe the Policy, since the collection and use of Personal Information is part of our everyday business providing services to our Customers. Likewise, we must ensure that we use the information we hold on our Crosby Associates Media Limited employees, temporary staff and contractors in accordance with the Applicable Privacy Law. This Policy sets out the standards that all those working in Crosby Associates Media Limited must adhere to.

2.8 Want more information?

If you want more information about data protection and how the rules affect Crosby Associates Media Limited, please contact Laura Bates.

3 The Data Protection Policy

We regard to the lawful and correct Processing of relevant Personal Information by Crosby Associates Media Limited as very important to successful operations and to maintaining confidence between those with whom we deal and ourselves. We ensure that our organisation treats Personal Information correctly and lawfully in accordance with the Applicable Privacy Law.

To this end, and among others, we fully endorse and adhere to the Principles of Data Protection, as set out in the Data Protection Act 1998 and in the terms set out below.

3.1 Breakdown of the Rules

3.1.1 Ensuring transparency

We must be transparent about the Personal Information that we hold on Individuals.

Understanding the Rule

Being open and transparent in the way organisations use and share Personal Information is an important step to demonstrate good data protection practices. Crosby Associates Media Limited is subject to this requirement in how we use Personal Information on Customers, clients, Crosby Associates Media Limited employees, suppliers, service providers, advisors, consultants, other professional experts, complainants and enquirers. As such, those Individuals should be properly notified about the uses of their Personal Information.

Practical Steps

Fair Processing information notices must be provided to [Customers and prospective Customers] and Crosby Associates Media Limited employees, if possible at the time of collection of that information or as soon as practicable after that.

3.1.2 Using Personal Information for a justifiable purpose only

We must only obtain and use Personal Information for purposes which are lawful and justifiable.

Understanding the Rule

Crosby Associates Media Limited must only collect the Personal Information of Individuals where it is relevant to the services that we provide to our Customers or to their relationship with

Crosby Associates Media Limited employees and contractors.

This rule means that we must identify and publicise the purposes for which Personal Information will be processed in in employment and contractor contracts.

Personal Information must not be used in a manner incompatible with the purpose for which it was obtained.

Practical Steps

When collecting Personal Information from Individuals, we must ensure that the fair Processing information notice made available to those Individuals (e.g. by way of the terms and conditions) contains all of the purposes for which the Personal Information may be used.

In addition, when collecting information, we must only collect those details which are necessary for the purposes for which that information is being obtained.

3.1.3 Ensuring data quality

We must keep Personal Information accurate and up to date.

Understanding the Rule

Processing inaccurate information can be harmful to Individuals and to Crosby Associates Media Limited. We must actively encourage Individuals to inform Crosby Associates Media Limited when their Personal Information changes.

Practical Steps

In the employment context, Crosby Associates Media Limited employees and temporary staff must remember to update their details (e.g. change of address).

All contractors and Customers must be actively encouraged to update their contact details by inviting them, when communication occurs, to notify us of any changes in their Personal Information.

3.1.4 Retaining data

We must keep Personal Information only for as long as is really necessary.

Understanding the Rule

Any Personal Information relating to Individuals should only be kept where there is a business or legal need to do so.

Practical Steps

Statutes or regulations may require that certain Personal Information be retained for a specified length of time, and it may also be prudent to keep certain Personal Information for a specific period so that we are able to defend properly any legal claims or manage an on-going business relationship.

Documents (including paper and electronic versions and e-mail) containing Personal Information must not be kept indefinitely and should always be deleted and destroyed once they have become obsolete or when that Personal Information is no longer required. Personal Information should not be retained simply on the basis that it might come in useful one day without any clear view of when or why.

3.1.5 Honouring Individuals' rights

We must always be receptive to any queries, requests or complaints made by Individuals in connection with their Personal Information and adhere to our Subject Access Request procedure.

Understanding the Rule

We will reply to queries and complaints in reasonable time and to the extent reasonably possible concerning the Processing of Personal Information by Crosby Associates Media Limited. We consider that the most important of all data protection rights is the ability of Individuals to access

Personal Information held about them. Individuals are entitled (by making a request to Crosby Associates Media Limited) to be supplied with a copy of any Personal Information held about them (including both electronic and paper records).

Other data protection rights include:

- Individuals may object to our use of their Personal Information.
- Individuals may ask us to change the information that we hold on them because they consider our information to be inaccurate or out-of-date.
- Individuals may ask Crosby Associates Media Limited to confirm that no decision taken by us is based solely on the Processing of their Personal Information by automatic means for the purpose of evaluating matters relating to them, for example, their creditworthiness.

Practical Steps

Where we receive a request from an individual exercising the right to access their information, we must follow the steps set out in our internal procedures.

Where we receive a request from an individual exercising any other data protection right we must notify the Data Protection Officer immediately.

3.1.6 Taking appropriate security measures

We must always adhere to appropriate technical and organisational security measures to protect Personal Information.

Understanding the Rule

Personal Information must be kept secure. Technical and organisational security measures are necessary to prevent the unauthorised or unlawful Processing or Disclosure of Personal Information and the accidental loss, destruction of, or damage to, Personal Information.

Practical Steps

We must monitor the level of security applied to a set of information, taking into account current standards and practices.

In particular, we must observe the security of information requirements set out in the Information Security Policy.

3.1.7 Using subcontractors

We must ensure that providers of services to us also adopt appropriate security measures.

Understanding the Rule

Where a provider of a service to Crosby Associates Media Limited has access to Personal Information of our current or prospective Crosby Associates Media Limited employees, temporary staff, contractors or Customers, we must impose contractual obligations dealing with the security of that information.

Practical Steps

We must always enter into a written contract with any service provider that processes Personal Information on our behalf. All contracts with providers of services should include the standard contractual provisions made available by the Data Protection Officer.

3.1.8 Ensuring adequate protection for overseas transfers

Transferring Personal Information outside the European Economic Area ("EEA") requires ensuring that the recipient provides the right level of protection.

Understanding the Rule

International transfers of Personal Information outside of the EEA are not allowed without appropriate steps being taken.

Practical Steps

Transferring any Personal Information outside the EEA requires taking appropriate legal steps such as contractual clauses. Please contact the Data Protection Officer if you are transferring Personal Information to service providers based outside the EEA.

3.1.9 Sensitive Personal Information: Safeguarding the use of sensitive Personal Information

We must only use sensitive Personal Information if it is absolutely necessary for us to use it.

Understanding the Rule

Sensitive Personal Information is information relating to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life and criminal convictions. This information deserves more stringent protection than other Personal Information, so our standards of care must be higher when dealing with this type of information.

Practical Steps

We must always assess whether sensitive Personal Information is essential for the proposed use.

We must only collect sensitive Personal Information when it is absolutely necessary in the context of our business and we must secure the individual's explicit consent to the collection and processing of sensitive Personal Information.

3.1.10 Legitimising direct marketing

We must always allow Customers to opt out of receiving marketing information.

Understanding the Rule

Another important data protection right that Individuals have is the right to object to the use of their Personal Information for direct marketing purposes and we must honour all such Opt-out requests where any direct marketing is carried out. This applies even where Individuals have previously opted-in to receiving direct marketing from us.

Practical Steps

We must ensure that the fair Processing information notice made available when Personal Information is collected includes the relevant mechanisms for collecting Individuals' consent to receiving marketing communications, and that it tells Individuals how they may change their marketing preferences. Please see the Data Protection Officer for further information.

3.1.11 Honouring Opt-outs

We must always suppress from marketing initiatives the Personal Information of Individuals who have opted out of receiving marketing information.

Understanding the Rule

It is essential that Customers' choices are accurately identified when any direct marketing campaigns are carried out. A failure to comply with an individual's Opt-out choice (e.g. by sending a mailing to an individual who has previously indicated to us that he or she does not wish to receive mailings) is likely to lead to complaints from the individual and possible scrutiny or enforcement action being taken by the relevant regulators.

Practical Steps

Where we are responsible for a direct marketing campaign, we must take all necessary steps to prevent the sending of marketing materials to Individuals who have opted out. In certain instances, it may also be necessary to obtain Opt-in consent from Individuals before sending them marketing communications. Please speak to the Data Protection Officer for further information.

3.2 Complying with the Rules

Why is it important that our employees comply with the Rules?

It is important that everyone within Crosby Associates Media Limited complies with the Rules, because we are all responsible for data protection compliance. A failure to comply with the rules could expose Crosby Associates Media Limited to regulatory and/or legal action which could mean the payment of compensation and/or fines. It may also result in significant reputational harm and brand damage for Crosby Associates Media Limited.

What happens if our employees breach a Rule?

If our employees breach a Rule, they should immediately inform their supervisor if they consider the breach to be sufficiently serious. If our employees are not certain whether the breach is serious, they are advised they should inform their supervisor in any event. Our employees are encouraged to always voluntarily tell us of any serious breaches, because we will consider any deliberate cover up or attempts to mislead us about a breach as a serious disciplinary matter.

Whilst we would always seek to work through any breach incident with our employees in order for them to understand the ramifications of their actions or omissions and continue to work on the same basis, regrettably, in some circumstances, we may have to commence disciplinary action against an employee if the breach is of a particularly damaging nature and, ultimately, we may have to terminate their contract.

Additionally, our employees are warned that knowingly or recklessly obtaining or disclosing Personal Information may be a criminal offence.

3.3 Training on the Rules

How can our employees receive training on the Rules?

All new joiners will receive training on the Rules. Existing Crosby Associates Media Limited employees and contractors will receive on-going training.

Can I receive refresher training on the Rules?

If our employees require any extra training or a refresher on any particular points, they can contact the Data Protection Officer. We will regularly run refresher training through the year, in addition to on-going training.

Auditing compliance with the Rules

We will audit compliance with the Rules and we will seek to understand why if any departments or teams fail to comply with the Rules. Once we have audited the requirements, we will prepare a remediation plan to ensure that the likelihood of any breach reoccurring is minimised. Should the remediation plan require you to take any actions, we expect you to co-operate fully].

3.4 Responsibilities

The role of the Data Protection Officer

The role of the Data Protection Officer comprises the following responsibilities:

- Preparation and annual review of this Policy.
- Ensuring compliance with Applicable Privacy Law by Crosby Associates Media Limited.
- Ensuring that Crosby Associates Media Limited have systems and controls in place to ensure on-going compliance and to evidence such compliance.
- Monitoring changes to Crosby Associates Media Limited's commercial activities and systems in order to ensure that any data protection compliance implications are identified and addressed.
- Monitoring the relevant regulators' websites and publications to identify and take appropriate actions to comply with any changes which may affect Crosby Associates Media Limited's compliance arrangements.
- Reviewing, amongst other things, all customer-facing documentation; marketing materials; employment contracts; terms and conditions; and Third Party contracts to ensure compliance with Applicable Privacy Law.
- Reviewing the necessary standards of staff awareness of their responsibilities, and those

of Crosby Associates Media Limited, under Applicable Privacy Law.

- Monitoring the effectiveness of staff training and the level of staff awareness of their responsibilities by preparing and carrying out a programme of periodic compliance monitoring, audits and relevant functions throughout Crosby Associates Media Limited.
- Promptly dealing with requests from Individuals.
- Reviewing administrative and resource matters.
- Ensuring that Crosby Associates Media Limited pays its annual notification renewal fee to the appropriate data protection authorities.
- Ensuring full co-operation with data protection authorities and other competent regulators.]

Reporting lines

The Data Protection Officer, the Head of HR and the Head of IT report on matters related to this Policy and the related policies directly to the Managing Directors as their line report.

CONFIDENTIAL