Data Protection Policy and Procedures

Updated: 26 April 2018

1. Introduction

Ethos Public Relations Limited (hereafter Ethos public relations) is committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of data for the purpose of providing public relations services to our clients, and for fulfilling product orders for our clients and through our online shop.

This data is collected and handled securely and Ethos public relations makes every effort to keep this data up to date. Emails and paper records are only stored for as long as they are needed or to comply with legal requirements. Records are then securely destroyed.

The Data Protection Act 1998 (DPA) and General Data Protection Regulations (GDPR) govern the use of information about people (personal data). Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs.

The Directors of Ethos public relations will remain the data controller for the information held. The Directors are responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. The Directors are required to read and comply with this policy.

2. Purpose

The purpose of this policy is to set out Ethos public relations' commitment and procedures for protecting personal data. Directors regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those we deal with. We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

The following are definitions of the terms used:

Data Controller – the Directors of Ethos public relations, who collectively decide what personal information Ethos public relations will hold and how it will be held or used.

Act means the Data Protection Act 1998 and General Data Protection Regulations – the legislation that requires responsible behaviour by those using personal information.

Data Subject – the individual whose personal information is being held or processed by Ethos public relations, for example a client employee, a client's customer or a customer of Ethos public relations' online shop.

Explicit consent – is a freely given, specific agreement by a Data Subject to the processing of personal information about her/him.

Explicit consent is needed for processing "sensitive data", which includes:

(a) Racial or ethnic origin of the data subject
(b) Political opinions
(c) Religious beliefs or other beliefs of a similar nature
(d) Trade union membership
(e) Physical or mental health or condition
(f) Sexual orientation
(g) Criminal record
(h) Proceedings for any offence committed or alleged to have been committed.

Information Commissioner's Office (ICO) – the ICO is responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies, but applies to named persons.

3. The Data Protection Act

This contains eight principles for processing personal data with which we must comply.

Personal data:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met

2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes

3. Shall be adequate, relevant and not excessive in relation to those purpose(s)

4. Shall be accurate and, where necessary, kept up to date

5. Shall not be kept for longer than is necessary

6. Shall be processed in accordance with the rights of data subjects under the Act

7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information

8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

4. Applying the Data Protection Act within Ethos public relations

Ethos public relations will let people know why we are collecting their data, which is for the purpose of carrying on our public relations work, or for distributing products for our clients or for selling products through our online shop. It is our responsibility to ensure the data is only used for these purposes. Access to personal information will be limited to Directors.

The personal data which may need to be held by Ethos public relations is: name, job title, address, phone number, mobile number, email address and gender. This data may be held on paper, emails, PCs, laptops, CDs, in archives or on smartphones.

The lawful basis for processing this data is:

- To undertake Ethos public relations business, including invoicing and customer liaison
- For client case studies and to promote our clients' businesses
- To fulfil clients' product orders
- To fulfil product orders from our online shop (http://www.ethos-pr.com/shop/)

Data held or used for other purposes incompatible with the original purpose will need consent to use it. Consents given before May 2018 will be re-acquired. We understand that Consent can be withdrawn at any time.

5. Responsibilities

The Directors of Ethos public relations are the Data Controller under the Act, and are legally responsible for complying with the Act, which means that they determine what purposes personal information held will be used for.

The Directors will take into account legal requirements and ensure that the Act is properly implemented and will, through appropriate management and the strict application of criteria and controls:

a) Collect and use information fairly
b) Specify the purposes for which information is used
c) Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements
d) Ensure the quality of information used
e) Ensure the rights of people about whom information is held can be exercised under the Act. These include:
    i. The right to be informed that processing is undertaken
    ii. The right of access to one's personal information
    iii. The right to prevent processing in certain circumstances
    iv. The right to correct, rectify, block or erase information which is regarded as wrong information
f) Take appropriate technical and organisational security measures to safeguard personal information
g) Ensure that personal information is not transferred abroad without suitable safeguards
h) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
i) Set out clear procedures for responding to requests for information.

The Directors of Ethos public relations are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

6. Procedures for Handling Data & Data Security

The Directors of Ethos public relations have a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

- Unauthorised or unlawful processing of personal data
- Unauthorised disclosure of personal data

- Accidental loss of personal data

The Directors of Ethos public relations must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper, in a computer or recorded by some other means e.g. tablet or smartphone.

Personal data relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data; however, combining various data elements such as a person's name and salary or religious beliefs etc. would be classed as personal data, and falls within the scope of the DPA.

The Directors of Ethos public relations consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and observe the guidance given below.

7. Procedures to Deal with a Data Breach

All organisations are required to report certain types of data breach to the ICO and in some cases to the individuals affected. A report to the ICO must be made within 72 hours (3 days) of becoming aware that an incident is reportable.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. We only have to notify the ICO where it is likely to result in a risk to individuals, for example, damage to reputation, financial loss, loss of confidentiality. If a data breach occurs, we will check whether anything could be done to avoid it happening again.

8. Operational Guidance

Email:

The Directors will consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved in the appropriate folder or printed and stored securely.

Emails that contain personal information no longer required for operational use, will be deleted from the personal mailbox and any "deleted items" box.

Phone Calls:

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions will be taken:

Personal information will not be given out over the telephone unless the Directors have no doubts as to the caller's identity and the information requested is innocuous. If the Directors have any doubts, they will ask the caller to put their enquiry in writing.

If Ethos public relations receives a phone call asking for personal information to be checked or confirmed, we will be aware that the call may come from someone impersonating someone with a right of access.

Laptops and Portable Devices:

All laptops and portable devices that hold data containing personal information will be protected with a suitable encryption program (password). Laptops and portable devices will be locked (password protected) when left unattended, even for short periods of time.

When travelling in a car, laptops will be kept is out of sight, preferably in the boot and if we have to leave a laptop in an unattended vehicle at any time, it will be put in the boot and we will ensure all doors are locked and any alarm set.

We will never leave laptops or portable devices in a vehicle overnight and we will never leave laptops or portable devices unattended in restaurants or bars, or any other venue.

When travelling on public transport, we will keep laptops and portable devices with us at all times and not in luggage racks or on the floor beside us.

Data Security and Storage:

We will store as little personal data as possible on our computers or laptops, only keeping those files that are essential. Personal data received on disk or memory stick will be saved to the relevant file on the computer or laptop. The disk or memory stick will then be securely returned (if applicable), safely stored or wiped and securely disposed of.

Ethos public relations insists on password protection for all devices used by our employees for the purposes of Ethos public relations business and on internet and malware security. Our computers are protected with BullGuard Internet Security.

Our computers and laptops will always be locked (password protected) when left unattended.

Passwords:

We will not use passwords that are easy to guess and we will not give out our passwords, write our passwords somewhere on a laptop or keep them written and stored in a laptop case.

Data Storage:

Personal data will be stored securely and will only be accessible to Ethos public relations Directors.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately. For financial records this will be seven years. For employee records see below. Archival material such as minutes and legal documents will be stored indefinitely. Other correspondence and emails will be disposed of when no longer required.

Ethos public relations will ensure that all personal data we hold is non-recoverable from any computer which has been passed on or sold to a third party.

Information Regarding Employees or Former Employees:

Information regarding former employees will be kept indefinitely. (If something occurs years later it might be necessary to refer back to a job application or other document to check what was disclosed earlier, in order that Directors comply with their obligations e.g. regarding employment law, taxation, pensions or insurance.)

Data Subject Access Requests:

Individuals have a right to make a Subject Access Request (SAR) to find out whether Ethos public relations holds their personal data, where, what it is used for and to have data corrected if it is wrong, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them.

Any SAR will be dealt with within 30 days. Steps will first be taken to confirm the identity of the individual before providing information, requiring both photo identification e.g. passport, and confirmation of address e.g. recent utility bill, bank or credit card statement.

If you are unhappy with the way Ethos public relations has handled your data, or you think that Ethos public relations has not dealt with your request for information properly, then you are entitled to complain to us – click here for our contact details. If you are still dissatisfied, then you are entitled to complain to the ICO (Information Commissioner's Office).

We may occasionally need to share data with other agencies which are not in furtherance of the work of Ethos public relations. The circumstances where the law allows Ethos public relations to disclose data (including sensitive data) without the data subject's consent include:

a. Carrying out a legal duty or as authorised by the Secretary of State protecting vital interests of a Data Subject or other person e.g. child protection
b. The Data Subject has already made the information public
c. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
d. Monitoring for equal opportunities purposes – e.g. race, disability or religion.

We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. We intend to ensure that personal information is treated lawfully and correctly.

Risk Management:

The consequences of breaching Data Protection can cause harm or distress to individuals if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Directors are aware that they can be personally liable if they use customers' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of Ethos public relations is not damaged through inappropriate or unauthorised access and sharing.

9. Privacy Notice

Ethos public relations uses personal data for the purpose of providing public relations services to our clients, and for fulfilling product orders for our clients and through our online shop.

Data may be retained for up to seven years for accounts purposes; information regarding former employees will be kept indefinitely; archival material such as minutes and legal documents will also be stored indefinitely. Other correspondence and emails will be disposed of when no longer required.

If you would like to find out more about how we use your personal data or would like to see a copy of information about you that we hold, please email info@ethos-pr.com.