CLASSACT

Building 435, Westcott Venture Park, Aylesbury, Buckinghamshire, HP18 0XB
Telephone: 01296 658222 – email: info@classact.uk.com

DATA PROTECTION POLICY

Context & Overview

Key Details.

- Policy Prepared By: Name: Thom Stretton Date: 26th September 2018 (Review)
- Approved By: Name: Mick Watson Date: 26th September 2018 (Review)
- Policy became operational on: Date: 25th May 2018
- Next Scheduled Review: Date: 25th February 2019

Introduction.

Class Act needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the company has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and comply with the law.

Why This Policy Exists.

This data protection policy ensures Class Act:

- Complies with data protection law and follows good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of data breach.

Data Protection Law.

General Data Protection Regulation (GDPR) comes into force on the 25th May 2018 and lays down the rules governing the collection, handling, storage and use of personal data.

These rules apply regardless of whether the data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

People, Risk and Responsibilities.

Policy Scope.

This policy applies to:

- The main offices of Class Act.
- All mobile installations of Class Act.
- All staff and volunteers of Class Act.
- All contractors, suppliers and other people working on behalf of Class Act.

It applies to all data that the company holds relating to identifiable individuals, even if that information is technically outside of General Data Protection Regulation (GDPR). This can include:

- Names of individuals.
- Postal addresses.
- Email addresses.
- Telephone numbers.
- Images of individuals.
- Plus, any other information relating to any individual(s).

Data Protection Risks.

This policy helps to protect Class Act from some very real data security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.
- **Failing to offer choice**. For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational Damage**. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities.

Everyone who works for or on behalf Class Act has some responsibility for ensuring data is collected, stored and handled appropriately.

Each group that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Proprietor, Mick Watson** is ultimately responsible for ensuring that Class Act meets its legal requirements.

- The **Data Protection Officer (DPO)** – Class Act Does not require a dedicated DPO.

- The **IT Manager, Thom Stretton,** is responsible for:

    - Ensuring all systems, services and equipment used for storing data meets acceptable security standards.

- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating and third-party services the company is considering using to store or process data. For instance, cloud-based computer services.
- Keeping the proprietor updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule – completed by 25th May 2018 in line with GDPR.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Class Act holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The **Marketing Manager, Michelle Thompson**, is responsible for:

  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other members of staff to ensure marketing initiatives abide by data protection principles.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work.**
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **Class Act will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines shown within this document.
- In particular; **strong passwords must be used,** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date or if no longer required, it should be updated or deleted and disposed of.
- Employees **should request help** if they are unsure about any aspect of data protection.
- **Photographs** of events **must not contain non-staff members** with the frame. Any event image showing individuals not employed by Class Act must be either deleted or edited to ensure that individuals cannot be identified.
- Class Act use 'Google Calendar' to keep employees and workers up to date with forthcoming events **no individual client or customer can be directly identified** with this environment.
- **Social Media** – Data is never to be extracted from any social media platform.
- Messages sent between members of Class Act will be done via 'What's App' **ensuring end-to-end encryption**.
- When not in use, **all paperwork with personal data** should be stored in the locked filing area. Care must be taken to ensure that paperwork is not observable through windows.
- **Non-staff members** must never be left unattended in the Class Act administration office.
- All paperwork with personal data must be shredded to dispose of, under no circumstance should paperwork of this nature be place in waste bins.

- Personal data stored electronically (with the exception of email .pst files) **must be stored in one secure location –** z:\\Avalon\class act documents. No personal data should be kept on individual desktops.

Social Media

Class Act will not use personal Data from social media platforms – such as Facebook, Instagram or Twitter – outside of the platform. No personal data will be extracted from social media platforms at any time for any reason.

Data Processing

Class Act have limited data processing activities they are:

- Gathering of email addresses from initial contact of a client, either by an incoming email, a completed form on our website, telephone or personal visit. This information is then stored electronically and in a 'event' file.
- The data is then only used to communicate with the client for their event, all notes and updates are stored in the same manner as above.
- The data is further used to generate invoices for payment of service rendered to the client.
- Once the event is complete all data is then archived in a secure area for record purposes.
- All email servers are reviewed and old file deleted on an annual basis.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT or Office Manager.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out:

- When not required, the paper or files should be kept in a **locked draw or filing cabinet**. Class Act has a one room administration area access to which is restricted to authorised personnel. Should visitors be granted access to this space they are to be **accompanied at all times**. When the space is vacated the door must be **locked separately to the building.**
- Employees should make sure that paper and printouts are **not left where unauthorised people could see them,** like on a printer or even through windows.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**.
- Data will not be uploaded to any **cloud computing service**.
- Servers containing personal data (Server - Avalon) should be **sited in a secure location**, away from the general office.
- Data is **backed up daily** to an off-site location (Server - Thanos)**.** Those backups should be tested regularly, in line with the company's standard backup procedures.

- Data should **never be saved directly** to laptops or other mobile devices like tablets or smartphones. Electronic calendar information that may be accessed from such devices will not carry any personal identifying information.
- All servers and computers containing data should be protected by **approved security software and a firewall.**

Data Use

Personal data is of no use to Class Act unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular; it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area.**
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.
- Under **no circumstances** will Class Act use personal data for marketing purposes..

Data Accuracy

The law requires Class Act to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Class Act should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance; by confirming a customer's details when they call.
- Class Act will make it **easy for data subjects to update the information** Class Act holds about them. For instance; via the company website.
- Data should be **updated as inaccuracies are discovered**. For instance; if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject Access Requests

All individuals who are the subject of personal data held by Class Act are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations.**

If individuals contact the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the DPO at *admin@classact.uk.com*. The DPO can supply a standard request form, although individuals do not have to do this.

Individuals will be charged £10.00 per subject access request. The DPO will aim to provide the relevant data within 14 days.

The DPO will always verify the identity of anyone making a subject access request before handing over any information.

If the DPO cannot confirm 'to their best knowledge' the identity of the individual making such a request, no information will be supplied.

Disclosing Data for Other Reasons

In certain circumstances, GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Class Act will disclose requested data. However, the DPO will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing Information

Class Act aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used.
- How to exercise their rights.

To this end, the company has a privacy statement, setting out how data relating to individuals is used by the company (Available at: https://www.classact.co/gdpr-privacy).

Last Reviewed: 26th September 2018