Worshipful Company of Builders' Merchants

Data Protection Policy

Addressing the General Data Protection Regulation (GDPR) 2018 [EU] and the Data Protection Act (DPA) 2018 [UK]

For information on this Policy or to request Subject Access please contact the Clerk.

Email: info@wcobm.co.uk

Phone: 020 7329 2189

Post: Worshipful Company of Builders' Merchants
4 College Hill
LONDON
EC4R 2RB

Definitions

The **Worshipful Company of Builders' Merchants ("the Company")** holds personal data about its employees, members, suppliers and other individuals for a variety of business purposes. This policy sets out how the Company seeks to protect personal data and ensure that officers of the Company understand the rules governing their use of personal data to which they have access in the course of their work.

Business purposes	The purposes for which personal data may be used by us: Membership management, event administration and financial management. *Business purposes include the following:* - *Compliance with legal and governance obligations and good practice* - *Ensuring privacy policies are adhered to (such as policies covering email and internet use)* - *Operational reasons, such as recording transactions, event planning and bookings, distribution of information and merchandise* - *Investigating complaints* - *Checking references, ensuring safe working practices, monitoring and managing access to administrative information* - *Promoting our industry* - *Improving services to members.*
Court	The Court of Assistants of the Company
GDPR	The General Data Protection Regulation 2016 (EU)
DPA	The Data Protection Act 2018 (UK)
Event	Any meeting, event, lecture, dinner, lunch, church service or other occasion organised by the Company for the benefit of its membership
Members/Membership	All Liverymen and Freemen of the Company
Personal data	Information relating to identifiable individuals, such as membership applicants, current and former members, employees, self-employed and other officers, suppliers and City and Livery contacts. *Personal data the Company gathers may include:*

	individuals' contact details, educational background, details of qualification certificates and diplomas, decorations held, education and skills, marital status, CV, job title and any special dietary requirements.
Sensitive personal data	*Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences or related proceedings is not requested, sought or held by the Company.*

Scope

This policy applies to all members of the Company. You must be familiar with this policy and comply with its terms.

This policy supplements any other policies relating to internet and email use. The Company may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be distributed to members.

Who is responsible for this policy?

The Company is not required to appoint a ***Data Protection Officer.*** The responsibility for this policy rests with the Court and it is maintained and administered by the Clerk and the Secretary as the Data Processors.

Procedures

Fair and lawful processing

The Company must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that the Company should not process personal data unless the individual whose details the Company is processing has given his/her consent.

The Data Processor's Responsibilities

- Keeping the Court updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection guidance and advice for all Court members and those included in this policy
- Answering questions on data protection from members, Court members and other stakeholders
- Responding to individuals such as members and suppliers who wish to know what data is being held on them by the Company
- Checking and approving with third parties that handle the Company's data, such as IT providers and caterers, any contracts or agreement regarding data processing
- Ensuring all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the Company is considering using to store or process data
- Approving data protection statements attached to emails and event notices.

The processing of all data must be:

- Necessary to deliver services to members
- In the legitimate interests of the Company and not unduly prejudicial the individual's privacy
- In most cases this provision will apply to routine membership and event data processing activities.

The Company's Data Protection Policy includes a Data Privacy Notice to Members and their guests on data protection.

The notice:

- Sets out the purposes for which the Company holds personal data on members and officers
- Highlights that the Company's work may require it to give information to third parties such as event venues and catering companies
- Provides that members have a right of access to the personal data that the Company holds about them.

Accuracy and relevance

The Company will ensure that any personal data it processes is accurate, adequate, relevant and not excessive, given the purpose for which it was

obtained. The Company will not process personal data obtained for one purpose for any unconnected purpose, unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that the Company correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Data Processor (the Clerk).

Your personal data

You must take reasonable steps to ensure that personal data the Company holds about you is accurate and updated as required. For example, if your personal circumstances change, you should inform the Clerk so that the data can be updated in the records.

Data security

The Company must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on behalf of the Company, the Clerk will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The Clerk must approve any cloud service used to store data
- Any servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the Company's backup procedures
- All servers containing sensitive data must be approved and protected by security software and a strong firewall.

Data retention

The Company will not retain personal data for any longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with data retention guidelines.

Subject access requests

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. This requirement is included in the GDPR 2018 and is expected to be included in the DPA 2018 Act.

Subject access requests from members or officers should be referred immediately to the Clerk (Data Processor).

Please contact the Clerk (Data processor) if you would like to correct or request information that the Company holds about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual's rights

The Company will abide by any request from an individual not to use their personal data for direct marketing purposes.

The Company will not send direct marketing material to someone electronically (e.g. via email) unless the Company has an existing business relationship with them in relation to the services being marketed.

GDPR 2018 provisions

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

Privacy Notice – transparency of data protection

Being transparent and providing accessible information to individuals about how their personal data will be used is important to the Company. The following are details on how the Company collects data and what it will do with it:

What information is being collected?	**Full name, address, age, telephone and email contact details, professional experience, interests as they relate to Company activities, any dietary or accessibility requests.**
Who is collecting it?	The Clerk and the Secretary to the Company.
How is it collected?	Membership application, event bookings, surveys.
Why is it being collected?	To process applications, arrange admissions and clothings, establish accurate event arrangements, to learn of members' interests and aspirations.
How will it be used?	To maintain a database, generate address labels, letters and emails, prepare ceremonies, book dinner numbers and request special diets and/or access requirements.
Who will it be shared with?	Within the Company: the Court and relevant Committees, including the Bursar and the Almoner. Outside the Company: the City Electoral register, the City Blue Book Directory and with affiliated organisations that organise events of interest to members, subject to member consent.
Identity and contact details of any data controllers	The Clerk and the Secretary are the data controllers. Their contact details are 020 7329 2189, or info@wcobm.co.uk.
Details of transfers to third country and safeguards	No information is transferred to a foreign country without the specific consent of those concerned at the time, should the need arise.
Retention period	Names, contact details and relevant Company admission, resignation and death dates are maintained in the database as a historical record of the Company's members.

Conditions for processing

The Company will ensure any use of personal data is justified, using at least one of the conditions for processing and this will be specifically documented. Those responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a Privacy Notice.

Justification for personal data

The Company will process personal data in compliance with the data protection principles set forth in the DPA.

Consent

The data that is collected by the Company is subject to active consent by the data subject. This consent can be revoked at any time.

Data portability

Upon request, a data subject will have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. The Data Processor (Clerk) will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers

No data may be transferred outside of the EEA without first discussing it with the Clerk (Data Processor). Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members have an obligation to report actual or potential data protection compliance failures that come to their notice. This allows the Company to:

- Investigate the failure and take remedial steps if necessary

- Maintain a register of compliance failures
- Notify the Information Commissioner's Office (ICO) of any compliance failures that are material either in their own right or as part of a pattern of failures.

Monitoring

Everyone must observe this policy. The Court has overall responsibility for this policy and will monitor it regularly to make sure it is being adhered to.

May 2018