# PRIVACY NOTICE FOR CLIENTS, CONTRACTORS & SUPPLIERS

**Effective from 25 May 2018/ Version 1**

**m a s t** a r c h i t e c t s

51 St Vincent Crescent
Glasgow G3 8NQ

Telephone: 0141 221 6834
Fax: 0141 221 8450
Email: mast@mastarchitects.co.uk

Web: www.mastarchitects.co.uk

# PRIVACY NOTICE FOR CLIENTS, CONTRACTORS & SUPPLIERS

In accordance with the General Data Protection Regulation (GDPR), we have implemented this privacy notice to inform you of the types of data we process about you. We also include within this notice the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data.

## A) DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing is fair, lawful and transparent
b) data is collected for specific, explicit, and legitimate purposes
c) data collected is adequate, relevant and limited to what is necessary for the purposes of processing
d) data is kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) data is not kept for longer than is necessary for its given purpose
f) data is processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g) we comply with the relevant GDPR procedures for international transferring of personal data

## B) TYPES OF DATA HELD

We keep several categories of personal data about you in order to carry out effective and efficient processes. We keep this data in a file relating to each contractor and we also hold the data within our computer systems, for example, our accounts systems.

Specifically, we hold the following types of data:

a) personal details such as name, address, phone numbers
b) bank account details
c) payment rates

## C) COLLECTING YOUR DATA

You provide several pieces of data to us directly during any contract negotiation period, for example your name and address, and subsequently upon the start of your engagement, for example, your bank details.

In some cases, we will collect data about you from third parties, such as intermediaries who may act as an introducer.

Personal data is kept in files or within the Company's HR and IT systems. All paper files that incorporate personal data are held securely in locked cabinets and access is restricted to senior management and administrators. The Company's IT system utilises a number of breach protection measures including Next Generation Application aware firewall, Intrusion Detection System configured and active on the firewall, Active Directory monitoring and alerting for failed access attempts and monitoring and alerting for new active directory account creation.

## D) LAWFUL BASIS FOR PROCESSING

The law on data protection allows us to process your data for certain reasons only. In the main, we process your data in order to comply with a legal requirement, in order to perform the contract we have with you or in pursuit of our legitimate interests.

The information below categorises the types of data processing we undertake and the lawful basis we rely on.

| Activity requiring your data | Lawful basis |
|---|---|
| Carry out the contract that we have entered into with you e.g. using your name, contact details | Performance of the contract |
| Ensuring you receive payment | Performance of the contract |
| Making decisions about who to enter into a contract with | Our legitimate interests |
| Business planning and restructuring exercises | Our legitimate interests |
| Dealing with legal claims made against us | Our legitimate interests |
| Preventing fraud | Our legitimate interests |
| Ensuring our administrative and IT systems are secure and robust against unauthorised access | Our legitimate interests |

## E) SPECIAL CATEGORIES OF DATA

Special categories of data are data relating to your:

a) health
b) sex life
c) sexual orientation
d) race
e) ethnic origin
f) political opinion
g) religion
h) trade union membership
i) genetic and biometric data.

Most commonly, we will process special categories of data when the following applies:

a) you have given explicit consent to the processing
b) we must process the data in order to carry out our legal obligations
c) we must process data for reasons of substantial public interest
d) you have already made the data public.

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations. However, we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time. There will be no consequences where consent is withdrawn.

## F) FAILURE TO PROVIDE DATA

Your failure to provide us with data may mean that we are unable to fulfil our requirements for entering into a contract with you or performing the contract that we have entered into.

## G) CRIMINAL CONVICTION DATA

We will only collect criminal conviction data where it is appropriate given the nature of the services you are to provide to us and where the law permits us. This data will usually be collected during contract negotiation, however, may also be collected during your engagement. We use criminal conviction data to determine your suitability, or your continued suitability for the engagement. We rely on the lawful basis of Performance of the Contract and our Legitimate Interests to process this data.

## H) WHO WE SHARE YOUR DATA WITH

Employees within our company who have responsibility for recruitment, administration of payment and contractual benefits and the carrying out performance related procedures will have access to your data which is relevant to their function. All employees with such responsibility have been trained in ensuring data is processing in line with GDPR.

Data is shared with third parties for the following reasons:

- To make payments to you and in respect of payments made by you to us.

We may also share your data with third parties as part of a Company sale or restructure, or for other reasons to comply with a legal obligation upon us. We have a data processing agreement in place with such third parties to ensure data is not compromised. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

We do not share your data with bodies outside of the European Economic Area.

## I) PROTECTING YOUR DATA

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such.

## J) RETENTION PERIODS

We only keep your data for as long as we need it for, which will be at least for the duration of your engagement with us though in some cases we will keep your data for a period after your engagement

has ended. Our retention period is 12 years especially in relation to data that is contractual in nature which from time to time may contain personal data.

## K) AUTOMATED DECISION MAKING

Automated decision making means making decision about you using no human involvement e.g. using computerised filtering equipment. No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

## L) DATA SUBJECT RIGHTS

You have the following rights in relation to the personal data we hold on you:

a) the right to be informed about the data we hold on you and what we do with it
b) the right of access to the data we hold on you. More information on this can be found in our separate policy on Subject Access Requests
c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification'
d) the right to have data deleted in certain circumstances. This is also known as 'erasure'
e) the right to restrict the processing of the data
f) the right to transfer the data we hold on you to another party. This is also known as 'portability'
g) the right to object to the inclusion of any information
h) the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate policy on your rights in relation to your data.

## M) CONSENT

Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

## N) MAKING A COMPLAINT

If you think your data rights have been breached, you are able to raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office - Scotland, 45 Melville Street, Edinburgh, EH3 7HL or by telephone on 0303 123 1115 (local rate) or by e-mail at Scotland@ico.org.uk.

## O) DATA PROTECTION COMPLIANCE

Our appointed compliance officer in respect of our data protection activities is:

Eilidh Jones
Eilidh@mastarchitects.co.uk

# DATA PROTECTION POLICY

**Effective from 25 May 2018/ Version 1**

**mast** architects

51 St Vincent Crescent
Glasgow G3 8NQ

Telephone: 0141 221 6834
Fax: 0141 221 8450
Email: mast@mastarchitects.co.uk

Web: www.mastarchitects.co.uk

# Data Protection Policy

## A) INTRODUCTION

We may have to collect and use information about people with whom we work. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources function as described below. It also covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

## B) DEFINITIONS

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

## C) DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing will be fair, lawful and transparent

b) data be collected for specific, explicit, and legitimate purposes
c) data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
d) data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) data is not kept for longer than is necessary for its given purpose
f) data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g) we will comply with the relevant GDPR procedures for international transferring of personal data

**D) TYPES OF DATA HELD**

We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

Specifically, we hold the following types of data:

a) personal details such as name, address, phone numbers
b) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, details on your education and employment history etc
c) details relating to pay administration such as National Insurance numbers, bank account details and tax codes
d) medical or health information
e) information relating to your employment with us, including:

    i) job title and job descriptions
    ii) your salary
    iii) your wider terms and conditions of employment
    iv) details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
    v) internal and external training modules undertaken

All of the above information is required for our processing activities. More information on those processing activities are included in our privacy notice for employees, which is available from your manager.

**E) EMPLOYEE RIGHTS**

You have the following rights in relation to the personal data we hold on you:

a) the right to be informed about the data we hold on you and what we do with it;
b) the right of access to the data we hold on you. More information on this can be found in the section headed "Access to Data" below and in our separate policy on Subject Access Requests";

c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
d) the right to have data deleted in certain circumstances. This is also known as 'erasure';
e) the right to restrict the processing of the data;
f) the right to transfer the data we hold on you to another party. This is also known as 'portability';
g) the right to object to the inclusion of any information;
h) the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate policy on employee rights under GDPR.

## F) RESPONSIBILITIES

In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed employees with responsibility for reviewing and auditing our data protection systems.

## G) LAWFUL BASES OF PROCESSING

We acknowledge that processing may be only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the employee's consent in order to process data.

However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Employees will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

## H) ACCESS TO DATA

As stated above, employees have a right to access the personal data that we hold on them. To exercise this right, employees should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in our Subject Access Request policy.

## I) DATA DISCLOSURES

The Company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

a) any employee benefits operated by third parties;
b) disabled individuals - whether any reasonable adjustments are required to assist them at work;
c) individuals' health data - to comply with health and safety or occupational health obligations towards the employee;
d) for Statutory Sick Pay purposes;
e) HR management and administration - to consider how an individual's health affects his or her ability to do their job;
f) the smooth operation of any employee insurance policies or pension plans;
g) to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

These kinds of disclosures will only be made when strictly necessary for the purpose.

## J) DATA SECURITY

All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

a) ensuring that data is recorded on such devices only where absolutely necessary.
b) using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
c) ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

## K) THIRD PARTY PROCESSING

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Company's commitment to protecting data.

## L) INTERNATIONAL DATA TRANSFERS

The Company does not transfer personal data to any recipients outside of the EEA.

## M) REQUIREMENT TO NOTIFY BREACHES

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available in our Breach Notification policy.

## N) TRAINING

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data compliance officers for the Company are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

## O) RECORDS

The Company keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities.

## P) DATA PROTECTION COMPLIANCE

Our appointed compliance officer in respect of our data protection activities is:

Eilidh Jones
eilidh@mastarchitects.co.uk