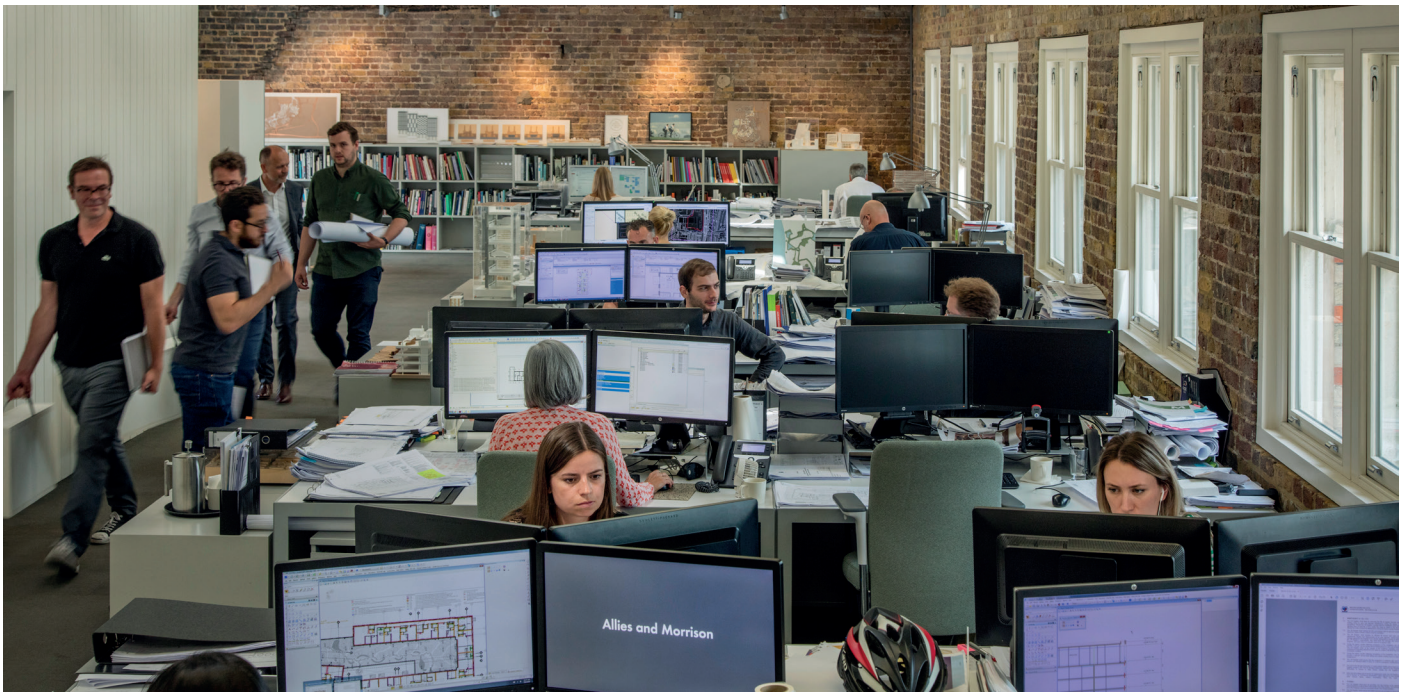
Allies and Morrison LLP
Privacy Policy



INTRODUCTION

This policy summarises the key points in relation to how Allies and Morrison collects, uses and discloses personal data and ensures compliance with General Data Protection Regulation (GDPR). Defined words are in the Appendix at the end of this policy.

WHAT IS PERSONAL DATA?

Personal data is information (including opinions) which relates to an individual and from which he or she can be identified either directly or indirectly through other data which the practice has or is likely to have in its possession. These individuals are sometimes referred to as data subjects.

RESPONSIBILITIES

Allies and Morrison is the Data Controller of personal data we process and therefore is responsible for ensuring our systems, processes, suppliers and people comply with data protection laws in relation to the information we handle.

All employees must abide by this policy when handling personal data and must take part in any required data protection training. Any breach will be taken seriously and may result in disciplinary action.

Joanna Bacon, Managing Partner, overseas compliance with data protection laws and our policy.

PRINCIPLES OF DATA PROTECTION

Allies and Morrison has adopted the GDPR principles to govern our use, collection and disclosure of personal data.

These principles provide that personal data must:

- be processed **fairly** and **lawfully** with valid and informed consent;
- be obtained for specific and **lawful purposes**;
- be kept **accurate** and **up to date**;
- be **adequate**, **relevant** and **not excessive** in relation to the purposes for which it is used;
- **not be kept for longer than is necessary** for the purposes for which it is used;
- be processed **in accordance with the rights of individuals**;
- be **kept secure** to prevent unauthorised processing and accidental loss, damage or destruction;
- and are not to be transferred to, or accessed from, another jurisdiction where these core principles cannot be met unless they can be adequately protected.

COLLECTION, USE AND DISCLOSURE

All data we collect and process falls into one of the following categories:-

- personal data relating to clients or other contacts;
- personal data obtained and created in relation to providing architectural or urban planning services; and
- personal data relating to our people.

How we collect and use personal data, for these three categories, is summarized below:

1. CLIENTS AND OTHER CONTACTS

Types of data
Information such as name and business information (email address, job title, who you work for).

Additional information may be processed where it is provided by you, for example in correspondence, on a business card, in connection with an event. This could include requests for and processing of data, for example, of dietary requirements which may reveal information about your health or religious beliefs.

Collection
Data is collected in our contact list databases as we receive your contact details.

You may request your profile data at any time to amend your information, to provide additional details or request that your personal data be removed from our databases.

Use
Personal data will be used to respond to any request you may make or to contact you.

Disclosure
Personal data:
- may be transferred worldwide to service providers who support the operation of the practice;
- which is shared with service providers will be limited to that which is required for providing our services and will be adequately protected;
- will not be given to other third parties without express permission.

2. IN PROVIDING ARCHITECTURAL OR URBAN DESIGN SERVICES

Types of data
Information processed for project management such as name, business information (email address, job titles, roles) and business identification documentation (e.g. Company registration numbers and VAT numbers).

Additional personal data may be processed when individuals are names in project matters on which we are providing professional services. Personal data may also be uploaded onto web based portals e.g. submissions, project websites, external sites.

Collection
Contact database information is collected from you directly. Further information (e.g. for due diligence purposes) may be collected from publicly available third party sources.

All additional personal data is collected when supplied to us, or created by us in connection with a particular matter on which we are providing services. Where relevant, this may be through a web based service you are using (e.g. a document control site).

Use
Contact database information is used for our architectural or urban design services, administration, commercial due diligence (e.g. credit checks) and as required by law (e.g. anti money laundering).

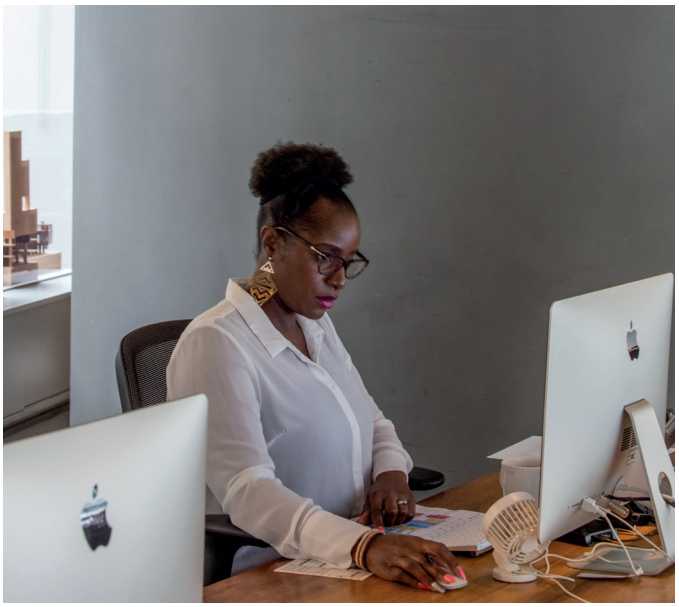
All other personal data will only be used for the purposes of providing our services and to comply with our statutory and regulatory obligations.

Disclosure
Personal data:
- may be transferred internationally to service providers who support the operation of our business;
- which is shared with service providers will be limited to that which is required for providing the service and will be adequately protected;
- will not be given to other third parties without express permission.

3. OUR PEOPLE
(Including applicants who apply for a job or a work placement with us)

Types of personal data
Personal data such as name, address, contact details, education and employment history; reference checks, passport copies

Collection
Personal data will be collected from a number of sources including your application and CV: by post, email, in person or through a third party; via reference providers and referees; via providers of occupational health services; by tracking your use of the practice's IT systems and information software; via notes and records kepth throughout your employment including absence records, questionnaires and surveys, performance reviews and details of any grievances and or disciplinary action, expense claims; CCTV security footage and swipe card data.



Use

Personal data will be used for:

- administration and management purposes, assessing suitability, eligibility and/or fitness to work, performance management, training and development, pay and remuneration, health and safety and the application, audit and enforcement of our policies and other terms and conditions relating to project working.

Disclosure

Your personal data:

- may be transferred to clients, and to service providers who support the operation of the practice;
- stored within the practice's information systems and within third party software applications and services which have been procured to support the operation of the HR function (e.g. AMPM Vantagepoint, Ideagen - all hosted in the EEA).
- transferred to other third parties such as our insurers, legal and other professional advisors, regulators, administrators and government departments, who may be acting as data controllers;
- shared with practice clients for the purposes of tendering for or providing architectural or urban planning services. When information is shared with service providers it is limited to that which is required for providing architectural and urban design services and will be adequately protected.

INDIVIDUALS' RIGHTS

Personal data must be processed in line with an individual's rights, including the right to:

- request a copy of their personal data;
- request that their inaccurate personal data is corrected;
- request that their personal data is deleted and destroyed when causing damage or distress.

Should you wish to make a request in line with your rights as an individual, please forward the request in writing or by email to Joanna Bacon, Managing Partner, jbacon@alliesandmorrison.com.

All employees must notify or inform Joanna Bacon immediately if they receive a request from a third party in relation to personal data which the practice processes.

How to make a complaint

You should direct all complaints relating to how the practice has processed your personal data to Joanna Bacon, Managing Partner, acting on behalf of Allies and Morrison (the Data Controller).

All Partners and employees must also inform Joanna Bacon, Managing Partner, acting on behalf of Allies and Morrison (the Data Controller) immediately if they receive a compliant relating to how the practice has processed personal data of a third party so the practice's complaints procedure may be followed.

Security

Information security is a key element of data protection. The practice holds Cyber Security Essentials Plus Certification and it is a requirement that all our people comply with the practice's IT Communications Policy. The practice takes appropriate measures to secure personal data and protect it from loss or unauthorised disclosure or damage.

We also utilise appropriate technological measures to transmit large or sensitive documents or data to clients and other third parties. However, we cannot be held responsible for the security of correspondence sent by email, fax, or post and or courier.

Transfer of Data

We use a number of suppliers in connection with the operation of our practice and they may have access to the personal data we process. For example, an IT supplier may see our personal data when providing software support, or a company which we use for event management may process contacts' personal data for us. When contracting with suppliers and or transferring personal data to a different jurisdiction, the practice takes appropriate steps to ensure that there is adequate protection in place and that the principles are adhered to.

Joanna Bacon
September 2021

Appendix Definitions

In the Privacy Policy, the following terms have the following meanings:

Allies and Morrison	means Allies and Morrison LLP
"client"	any person or organisation to whom the practice provides a service and who is identified as a client on the practice's practice databases, regardless of whether time is recorded or a fee is charged;
"contact"	an individual who is a contact of the practice, including any client, any potential or former client, any supplier, any consultant, or any another professional advisor and any other contact of the practice;
"AMPM"	is the practice's client relationship management system (CRM) and project related database;
"data"	recorded information whether stored electronically, on a computer, or in certain paper-based filing systems;
"Data Controller"	a person who or an organisation which determines how personal data is processed and for what purposes.
"individual" or "you"	the person whose personal data is being collected, held or processed;
"IT Communications Policy"	The practice's IT Communications Policy;
"personal data"	please see the 'what is personal data' section of this policy;
"our people"	means Partners, consultants, employees, temporary workers, agency and casual workers, contractors, collaborators, volunteers, and those on work placements providing services to or working for the practice;
"policy"	the Privacy Policy as amended from time to time;
"principles"	the core data protection principles set out in the Privacy Policy
"process" or "processing"	any activity that involves use of personal data. It includes obtaining, recording or holding the personal data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties as a result of those third parties having access to it.