MAPP

Author	**Sean Greathead, Jonathan Gill and Rob Stark**
Document Name	**Internal Corporate GDPR Policy**
Date original policy came into effect	**15th April 2017**
Changes since the previous version	**Minor Adjustments (Typos and Titles) and Updating of Timelines**
Date for completion of next review	**31st August 2021**

This policy sets out MAPP's commitment to data protection, and individual rights and obligations in relation to personal data.

Introduction **2**
Purpose 2
Data Protection Principles **3**
Individual rights 4
Subject access requests 4
Other Rights 5
Data security **5**
Data breaches 6
Individual responsibilities **6**
Training 7
Law relating to this document **7**
Form for making a subject access request (compliant with the GDPR) **8**
Employee Notice Wording **10**
What information does the organisation collect? 10
Why does the organisation process personal data? 11
Who has access to data? 12
How does the organisation protect data? 12
Your rights 13
What if you do not provide personal data? 13

Automated decision-making 14

Job Applicant Privacy Notice (Compliant with the GDPR) Notice Wording: 15

What information does the organisation collect? 15

Why does MAPP process personal data? 16

Who has access to data? 16

How does MAPP protect data? 17

For how long does MAPP keep data? 17

Your rights 17

What if you do not provide personal data? 18

Automated decision-making 18

Introduction

Purpose

MAPP is committed to being transparent about how it collects and uses the personal data of prospective employees, current employees, interns and ex-employees, and to meeting its data protection obligations. This policy sets out MAPP's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, interns, apprentices, work experience participants] and former employees, referred to as HR-related personal data. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

MAPP has appointed the Chief of Staff as its Internal Corporate Data Compliance Officer. This role is to inform and advise MAPP on its data protection obligations. They can be contacted at **datacompliance@wearemapp.com**. Questions about this policy, or requests for further information, should be directed to the data compliance officer.

Definitions

Personal Data: This refers to any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

Sensitive Personal Data: This means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

Criminal Records Data: This means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data Protection Principles

MAPP processes HR-related personal data in accordance with the following data protection principles:

- MAPP processes personal data lawfully, fairly and in a transparent manner.
- MAPP collects personal data only for specified, explicit and legitimate purposes.
- MAPP processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- MAPP keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- MAPP keeps personal data only for the period necessary for processing.
- MAPP adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

MAPP tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where MAPP processes sensitive personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on sensitive personal data and criminal records data.

MAPP will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate. MAPP enables individuals to change their data themselves in as many instances as possible via the self service feature of our HR Information System.

Personal data gathered during the contractual relationship, is held in the individual's personnel file (electronic format), and on HR systems. The periods for which the organisation holds HR-related personal data are contained in its privacy notices to individuals.

MAPP keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, MAPP will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

MAPP will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

To make a subject access request, the individual should send the request to **datacompliance@wearemapp.com**. In some cases, MAPP may need to ask for proof of identification before the request can be processed. MAPP will inform the individual if it needs to verify his/her identity and the documents it requires.

MAPP will normally respond to a request within a period of one month from the date it is received. In some cases, such as where MAPP processes large amounts of the individual's data, it may respond within three months of the date the request is received. MAPP will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, MAPP is not obliged to comply with it. Alternatively, MAPP can agree to respond but will charge a fee, which will be based on the

administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which MAPP has already responded. If an individual submits a request that is unfounded or excessive, MAPP will notify him/her that this is the case and whether or not it will respond to it.

Other Rights

Individuals have a number of other rights in relation to their personal data. They can require MAPP to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the MAPP's legitimate grounds for processing data (where MAPP relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override MAPP's legitimate grounds for processing data.

To ask the organisation to take any of these steps, the individual should send the request to **datacompliance@wearemapp.com**.

Data security

MAPP takes the security of HR-related personal data seriously. MAPP has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. These controls include employee access requirements being determined upon appointment and authorised by an appropriate senior manager; user groups are created for each system and role to enforce appropriate segregation of duties; data recovery and disaster recovery procedures are in place to ensure data cannot be erased accidentally or without proper authority.
Where MAPP engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Data breaches

If MAPP discovers that there has been a reportable breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Individual responsibilities

Individuals are responsible for helping MAPP keep their personal data up to date. Individuals should let MAPP know if data provided to MAPP changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals and of our clients, tenants and suppliers in the course of their employment,, internship or apprenticeship. Where this is the case, MAPP relies on individuals to help meet its data protection obligations to staff, clients, tenants and suppliers.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside MAPP) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- to undertake and complete all relevant training regarding IT security and data protection issued by the company;
- not to remove personal data, or devices containing or that can be used to access personal data, from MAPP's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Further details about MAPP's security procedures can be found in the IT security policy.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under MAPP's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

MAPP will provide training to all individuals about their data protection responsibilities as part of the induction process. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Law relating to this document

General Data Protection Regulation (2016/679 EU)
Data Protection Bill

MAPP

Form for making a subject access request (compliant with the GDPR)

Name:
Daytime telephone number:
Email:
Address:
Employee number:
By completing this form, you are making a request under the General Data Protection Regulation (GDPR) for information held about you by the organisation that you are eligible to receive.
Required information (and any relevant dates):

[Example: Emails between "A" and "B" from 1 May 2017 to 6 September 2017.]
By signing below, you indicate that you are the individual named above. The organisation cannot accept requests regarding your personal data from anyone else, including family members. We may need to contact you for further identifying information before responding to your request. You warrant that you are the individual named and will fully indemnify us for all losses, cost and expenses if you are not. Please return this form to one of the People team or email to datacompliance@wearemapp.com. Please allow 30 days for a reply.
Data subject's signature:
Date:

Employee Notice Wording

Data controller: MAPP Ltd/MAPP Retail LLP 180 Great Portland Street, London W1W 5QS
Data Compliance Officer: Jonathan Gill - datacompliance@wearemapp.com

The organisation collects and processes personal data relating its employees to manage the employment relationship. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the organisation collect?

The organisation collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- information about your criminal record if you have one;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

MAPP may collect this information in a variety of ways. For example, data might be collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, MAPP may collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law.
Data will be stored in a range of different places, including in your personnel file, in the organisation's HR management systems and in other IT systems (including the organisation's email system).

Why does the organisation process personal data?

The organisation needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefits, pension and insurance entitlements.
In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.
In other cases, the organisation has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;

- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- provide references on request for current or former employees;
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace.

Sensitive personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities).

Where MAPP processes sensitive personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring.

Who has access to data?

Your information may be shared internally, including with members of the HR and recruitment team (including payroll), your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles.
The organisation shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service. The organisation may also share your data with third parties in the context of a sale of a transfer of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.
The organisation also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of benefits and the provision of occupational health services.
MAPP will not transfer your data to countries outside the European Economic Area.

How does the organisation protect data?

The organisation takes the security of your data seriously. The organisation has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where the organisation engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.
For how long does the organisation keep data?
MAPP will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are as follows:

- Learning Records: 7 Years
- HRIS Records: 7 Years
- Performance Management Records: 3 Years
- Employee File: 3 Years
- Email Account: 5 Years
- Payroll Information: 7 Years
- Employment History (ie Length of Service and Title): Indefinitely for Referencing Purposes.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing.

[If you would like to exercise any of these rights, please contact Jonathan Gill (**datacompliance@wearemapp.com**)

If you believe that MAPP has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You have some obligations under your employment contract to provide the organisation with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory

leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the organisation to enter a contract of employment with you. If you do not provide other information, this will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Automated decision-making

Employment decisions are not based solely on automated decision-making.

Job Applicant Privacy Notice (Compliant with the GDPR) Notice Wording:

Data controller: MAPP (Property Management) Ltd / MAPP Retail LLP 180 Great Portland Street, London W1W 5QS
Internal Corporate Data Compliance Officer: Jonathan Gill - **datacompliance@wearemapp.com**

As part of any recruitment process, MAPP collects and processes personal data relating to job applicants. MAPP is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

The Privacy Statement for Job Applicants can be found on the MAPP Website as follows: https://www.wearemapp.com/privacy-policy/

What information does the organisation collect?

MAPP collects a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements;
- whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process;
- information about your entitlement to work in the U and this includes copies of the relevant proof thereof; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

MAPP may collect this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment, including online tests.

MAPP may also collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks.

Data will be stored in a range of different places, including on your application record, in HR management systems, Applicant Tracking System and on other IT systems (including email).

Why does MAPP process personal data?

MAPP needs to process data to take steps at your request prior to entering into a contract with you. It may also need to process your data to enter into a contract with you. In some cases, MAPP needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

MAPP has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows MAPP to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. MAPP may also need to process data from job applicants to respond to and defend against legal claims.

MAPP may process information about whether or not applicants are disabled to make reasonable adjustments for candidates who have a disability. This is to carry out its obligations and exercise specific rights in relation to employment.

Where MAPP processes sensitive personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is for equal opportunities monitoring purposes.

For some roles, MAPP is obliged to seek information about criminal convictions and offences and financial conduct. Where the organisation seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.

If your application is unsuccessful, MAPP may keep your personal data on file in case there are future employment opportunities for which you may be suited. MAPP will ask for your consent before it keeps your data for this purpose and you are free to withdraw your consent at any time.

Who has access to data?

Your information may be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

MAPP will not share your data with third parties, unless your application for employment is successful and it makes you an offer of employment. MAPP will then share your data with former employers to obtain references for you, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.

MAPP will not transfer your data outside the European Economic Area as a job applicant.

How does MAPP protect data?

MAPP takes the security of your data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties. There is restricted access to all relevant data through two factor authentication and restriction of distribution of information.

For how long does MAPP keep data?

If your application for employment is unsuccessful, MAPP will hold your data on file for 12 months after the end of the relevant recruitment process. If you agree to allow MAPP to keep your personal data on file, MAPP will hold your data on file for a further 12 months for consideration for future employment opportunities. At the end of that period or once you withdraw your consent, your data is deleted or destroyed, unless you request for MAPP to retain your information.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file, but also retained in the Applicant Tracking System for record purposes and retained during your employment. The periods for which your data will be held will be provided to you in a new privacy notice.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require MAPP to change incorrect or incomplete data;
- require MAPP to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where MAPP is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact Jonathan Gill (**datacompliance@wearemapp.com**)

If you believe that MAPP has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to MAPP during the recruitment process. However, if you do not provide the information, MAPP may not be able to process your application properly or at all.

Automated decision-making

Recruitment processes are not based solely on automated decision-making.