DATA PROTECTION & PRIVACY POLICY

CONTENTS

1. Introduction

McArthurGlen understands the value of personal data and greatly respects the privacy of our customers, colleagues, partners and suppliers. Through this Policy we seek to uphold the highest possible standards in our approach to data protection in order to comply with our obligations and ensure the security of the data entrusted to us.

We collect and process data from various sources. As a business we have a responsibility to ensure that this data has been collected, stored, used and destroyed in accordance with all relevant data protection legislation. There are significant risks associated with data loss. The McArthurGlen Data Protection and Privacy Policy (the Policy) is intended to ensure compliance with the law, prevent harmful and embarrassing data breaches; protect our reputation and the goodwill of our customers, brand partners and investors.

This Policy sets out how personal data should be collected, stored, secured, transferred and destroyed. It applies to all colleagues working for, or on behalf of, McArthurGlen in any capacity including:

- Employees at all levels;
- Directors;
- Officers;
- Agency workers;
- Seconded workers;
- Volunteers;
- Interns;
- Agents;
- Contractors; and
- Within the limits in which comparable provisions of law apply to them, anyone who could have access to personal data collected by, or on behalf of, McArthurGlen.

All colleagues are requested to read, understand and comply with this Privacy Policy when processing personal data on behalf of McArthurGlen. Any queries or comments should be referred to the Data Protection Officer *McArthurGlen@dataprotectionpeople.com* or a member of the UK Legal Team.

1.1 Definitions:

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes which they, by a statement or by a clear positive action, signify agreement to the processing of personal data relating to them.

Data Controller: the person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in line with the GDPR. McArthurGlen is the data controller of all personal data relating to our personnel and personal data used in our business for our own commercial purposes.

Data Subject: a living, identifiable individual about whom we hold personal data.

Data Protection Officer (DPO): the person appointed in specific circumstances under the GDPR with responsibility for data protection compliance.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal data is subject to the legal safeguards specified in the GDPR.

Personal data: any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess

or can reasonably access. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Personal data specifically includes, but is not limited to:

- Personal contact details such as name, title, addresses, telephone numbers, and email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date.
- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as swipecard records.
- Information about use information and communications systems.
- Mac address.
- Photographs.

Personal data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Impact Assessment (PIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of 'privacy by design' and should be conducted for all major system or business change programs involving the processing of personal data.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals

(for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the Company's policies, operating procedures or processes related to this Privacy Policy and designed to protect personal data, available *here*.

Sensitive Personal data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and personal data relating to criminal offences and convictions.

2. Responsibilities

McArthurGlen understands that the correct and lawful treatment of personal data will maintain confidence in our organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take very seriously at all times. In addition, businesses are exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

All colleagues are responsible for ensuring they comply with this Policy and need to ensure they adhere to the appropriate practices, processes, controls put in place to safeguard personal data within our business.

The Data Protection Officer is responsible for overseeing this Privacy Policy and, as applicable, developing related Policies and guidelines and can be reached at *McArthurGlen@dataprotectionpeople.com*.

Please contact the Data Protection Officer with any questions about the operation of this Policy or the GDPR, or if you have any concerns that this Policy is not being or has not been followed.

Colleagues must always contact the Data Protection Officer in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process personal data (including the legitimate interests used by the Company);

(b) if you need to rely on consent and/or need to capture explicit consent;

(c) if you need to draft a Privacy Notice;

(d) if you are unsure about the retention period for the personal data being processed;

(e) if you are unsure about what security or other measures you need to implement to protect personal data;

(f) if there has been a personal data breach;

(g) if you are unsure on what basis to transfer personal data outside the EEA;

(h) if you receive and or need any assistance dealing with any rights invoked by a data subject;

(i) whenever you are engaging in a significant new, or change in, processing activity which is likely to require a *PIA* or plan to use personal data for purposes others than what it was collected for;

(j) if you need help complying with applicable law when carrying out direct marketing activities;

(k) if you need help with any contracts or other areas in relation to sharing Personal data with third parties (including our vendors)

3. Personal data protection principles

McArthurGlen adheres to the principles relating to processing of personal data set out in the GDPR which require personal data to be:

(a) Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency).

(b) Collected only for specified, explicit and legitimate purposes (purpose limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation).

(d) Accurate and where necessary kept up to date (accuracy).

(e) Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (storage limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (security, integrity and confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (transfer limitation).

(h) Made available to data subjects and data subjects allowed to exercise certain rights in relation to their personal data (data subject's rights and requests).

4. Lawfulness, fairness, transparency

4.1 Lawfulness and fairness

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

McArthurGlen may only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing but ensure that we process personal data fairly and without adversely affecting the data subject.

The GDPR allows processing for specific purposes, some of which are set out below:

(a) the data subject has given his or her consent;

(b) the processing is necessary for the performance of a contract with the data subject;

(c) to meet our legal compliance obligations;

(d) to protect the data subject's vital interests;

(e) to pursue our legitimate interests for purposes where these do not override the interests or fundamental rights and freedoms of data subjects.

4.2 Consent

A data subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing – such as opt-in tick boxes. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Where consent is relied upon as the lawful basis of data processing (e.g. for inclusion in the CRM data base for marketing purposes) data subjects must be easily able to withdraw their consent at any time. Withdrawal must be promptly honoured. Please note that consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented.

Colleagues will need to evidence consent captured and keep records of all consents so that McArthurGlen can demonstrate GDPR compliance.

4.3 Transparency – Privacy Notices

The GDPR requires data controllers to provide detailed, specific information to data subjects when data is collected from the data subject. Such information is provided through an appropriate 'Privacy Notice'. Privacy notices must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand them.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we must provide the data subject with a privacy notice detailing all the information required by the GDPR. Including the identity of the data controller and Data Protection Officer, how and why we will use, process, disclose, protect and retain that personal data. **Please note that the privacy notice must be presented when the data subject first provides the personal data.**

When Personal data is collected indirectly (for example, from a third party or publicly available source), the data subject must be provided with all the information required by the GDPR as soon as possible after collecting/receiving the data.

5. Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

6. Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Colleagues may only process personal data when necessary for the performance of their job duties. Please do not collect 'excessive data'. When personal data is no longer needed for the specified purposes, it is must be deleted or anonymised in accordance with the McArthurGlen Data Retention Policy.

7. Accuracy

The GDPR requires personal data be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. Please ensure that the personal data you use and hold is accurate, complete, kept up to date and relevant to the purpose for which it was collected. All reasonable steps must be taken to destroy or amend inaccurate or out-of-date personal data.

8. Data retention

Personal data should not be kept in an identifiable form for longer than is necessary for the purpose of processing. Where there is no longer a legitimate business purpose for processing data e.g for legal, accounting or reporting requirements, personal data must be deleted or anonymised. McArthurGlen Data Retention Policy sets out retention requirements.

9. Security integrity and confidentiality

9.1 Protecting personal data

As a business we must guard against loss, theft or damage to personal data. In order to protect our personal data, McArthurGlen colleagues are asked to uphold the following security measures:

(a) Entry controls - any stranger seen in entry-controlled areas should be reported.
(b) Secure lockable desks and cupboards - desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
(c) Methods of disposal - paper documents containing confidential information should be disposed of in the confidential waste bins or shredded. Digital data should be physically destroyed when they are no longer required. The IT department will advise as to the most appropriate method of disposal/erasure.
(d) Equipment – monitors showing confidential information should not be visible to passers-by. Colleagues are reminded to lock screens or log off from their PC and laptops when they are left unattended.
(e) Any sensitive data, whether it be personal or business sensitive, should be filed clearly so that it can be located by users, and password protected or encrypted so that only permitted individuals can view the data.
(f) Data subject information, highly sensitive or confidential information sent via email or held on computer must be identified as such and password protected. Encrypted equipment should be used by those holding information of a sensitive nature for any data subject. The DPO will liaise with each department to assist with identification of where encrypted equipment is necessary.
(g) Colleagues may only transfer personal data to third-party providers who agree to comply with GDPR requirements and agree to put adequate security in place as requested.

McArthurGlen will also secure personal data by appropriate technical and organisational measures. Colleagues must follow the procedures and technologies put in place to maintain the data security from the point of collection to the point of destruction. Colleagues must comply with the McArthurGlen Information Security Policy and not attempt to circumvent the administrative, physical and technical safeguards we implement in accordance with the GDPR to protect personal data.

9.2 Reporting a personal data breach

The GDPR requires data controllers to notify any personal data breach to the applicable regulator and, in certain instances, the data subject.

If colleagues know or suspect that a personal data breach has occurred, do not attempt to investigate the matter independently. Please contact the Data Protection Officer *McArthurGlen@dataprotectionpeople.com* and the legal department *MGUK.LegalDept@mcarthurGlen.com* immediately. **All evidence relating to the potential personal data breach should be preserved in line with the *Data Breach Protocol* .**

10. Transfer limitation

The GDPR restricts data transfers to countries outside the EEA.

Personal data may only be transferred outside of the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard model contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Data Protection Officer;

(c) the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

As a rule McArthurGlen does not transfer data outside of the EEA. Any proposals to do so must be addressed with the Data Protection Officer and the Legal Department beforehand.

11. Data subject's rights and requests

Data subjects have a number of rights when it comes to how we handle their personal data. These include rights to:

(a) withdraw consent to processing at any time;

(b) receive certain information about the data controller's processing activities;

(c) request access to their personal data that we hold;

(d) prevent our use of their personal data for direct marketing purposes;

(e) ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict processing in specific circumstances;

(g) challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which personal data is transferred outside of the EEA;

(i) prevent processing that is likely to cause damage or distress to the data subject or anyone else;

(j) be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

(k) make a complaint to the supervisory authority; and

(l) in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

Colleagues must verify the identity of an individual requesting data under any of the rights listed above. Do not allow third parties to persuade you into disclosing personal data without proper authorisation. Please discuss any data subject requests with the Data Protection Officer or the Legal Department if in doubt.

12. Accountability

12.1 McArthurGlen is responsible for, and must be able to demonstrate, compliance with the data protection principles through adequate resource and controls. We will do this in the following ways:

(a) Appointment of a suitably qualified Data Protection Officer and an executive accountable for data privacy. The Compliance Committee will take this role;

(b) implementing privacy by design when processing personal data and completing Privacy Impact Assessments where processing presents a high risk to rights data subjects;

(c) integrating data protection into internal documents including this Policy, related policies and privacy notices;

(d) regularly training colleagues on the GDPR, this Policy, related policies and data protection matters;

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement efforts.

12.2 Record keeping and the Data Processing Register

The GDPR requires data controllers to keep full and accurate records of all our data processing activities.

The Data Processing Register includes the name and contact details of the data controller and the Data Protection Officer, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data retention period and a description of the security measures in place. The *Data Processing Register* is held centrally and colleagues must ensure this register is kept up to date at all times.

12.3 Training and audit

McArthurGlen are required to ensure all colleagues have undergone adequate training to enable them to comply with data privacy laws. Our systems and processes will also be stress tested on a regular basis to assess compliance. Colleagues are required to review the systems and processes under their control to ensure they comply with this Policy. Any concerns must be flagged immediately with the Data Protection Officer, *McArthurGlen@dataprotectionpeople.com*, who will advise accordingly.

12.4 Privacy by design and Privacy Impact Assessment (PIA)

The GDPR requires data controllers to implement 'privacy by design' measures when processing personal data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

Colleagues must assess what privacy by design measures can be implemented on all programs/systems/processes that process personal data by taking into account the following:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of processing; and

(d) the risks and severity of impact for rights of data subjects.

Data controllers must also conduct *Privacy Impact Assessments* in respect to high risk processing.

Colleagues must conduct a PIA when implementing major system or business change programs involving the processing of personal data including:

(e) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(f) Automated Processing including profiling;

(g) large scale Processing of sensitive data; and

(h) large scale, systematic monitoring of a publicly accessible area.

A PIA must include:

(i) a description of the processing, its purposes and the data controller's legitimate interests if appropriate;

(j) an assessment of the necessity and proportionality of the processing in relation to its purpose;

(k) an assessment of the risk to individuals; and

(l) the risk mitigation measures in place and demonstration of compliance.

PIA findings must be discussed with the Data Protection Officer before new systems or change are implemented.

12.5 Direct marketing

McArthurGlen is subject to certain rules and privacy laws when marketing to our customers. For example, a data subject's prior consent is required for electronic direct marketing (for example, by email or text). The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information. A data subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

12.6 Sharing Personal data

Data controllers are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

Colleagues may only share the personal data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the personal data complies with the privacy notice provided to the data subject and, if required, the data subject's consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

The personal data we hold may only be shared internally with another employee, agent or representative of McArthurGlen Group if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

13. Changes to this Privacy Policy

McArthurGlen reserves the right to change this Privacy Policy at any time without notice to colleagues. Please check back regularly to obtain the latest copy of this Policy.