Secondee Privacy Notice

1. Introduction

This Privacy Notice is in addition to the Employee Privacy Notice. It applies to current and former employees, workers, agency workers, consultants, interns, partners and directors who have been seconded to another country of work under global mobility (together referred to as 'Secondees', 'you' or 'data subject' in this document).

Marshall is the "data controller" for the purposes of data protection law. This means that we are responsible for deciding how we hold and use personal information. We are required by law to notify you of the information contained in this Secondee Privacy Notice.

It is important that you retain and read this document.

We may update this document at any time and the latest version will always be available on the Company Internet, but we will send you a new Secondee Privacy Notice if any significant changes are made. A paper copy of this can be obtained on request from HR Support.

2. Responsibilities

2.1 The Global Mobility Specialist is responsible for ensuring that this notice is made available to data subjects prior to Marshall deploying them.

2.2 All Employees/Staff of Marshall who interact with data subjects are responsible for ensuring that this notice is drawn to the data subject's attention.

3. Privacy Notice

3.1 We are

Marshall Group. Please refer to your main privacy notice for full details of companies covered by this title.

Our Data Privacy Manager and HR can be contacted directly here:

- HR.support@marshalladg.com (Marshall HR Department)
  01223 373120
- DataPrivacyManager@Marshalladg.com (Marshall Data Privacy Manager)
  01223 373206

Any queries referring to the Secondee Privacy Notice should be referred to HR in the first instance.

3.2 Types of Personal data:

Is any data that could identify a living individual. Please refer to your Employee Privacy Notice for full details of definitions

3.3 We <u>will</u> collect and process the following personal data about you:

Ordinary personal data

- Surname, First Name, Middle Name, Job Title, address, Salary and other renumerations and benefits.

3.4 We <u>may</u> collect and process the following personal data about you:

The Personal Identifiable Information we *may* use is:-

Ordinary personal data

- Surname, First Name, Middle Name, Nationality, Citizenship, Date of Birth, Place of Birth, Gender/Sex, Telephone No, Mobile Telephone No.

  Passport No, Date of issue, Date of expiry, Passport photo, Issueing Authority, your signature.

- National ID Card No., Place of Issue, File No, Occupation/Profession, Sponsor, Date of issue, Date of expiry.

- Residence No, Expiry Date

- Driving License No, Issue Date, Expiry Date, Place of Issue, Licensing Authority

- Medical Insurance Member No, Issue Date, Expiry Date, Policy Holder Name, Cover held.

- Job Role for purposes of residency, Salary in country of deployment, place of work

- Information relating to your qualifications e.g qualifications attained, issuing authority,
- Information relating to your educational history
- Marital status
- Bank details in country of deployment
- Bank details in country of origin
- Occupational history
- Any names you have previously been known by.
- Any online Ids you are or have been previously known by.

Special category personal data

- Religion
- Ethnicity
- Genetic identifier such as finger or hand print or a retinal scan.

3.5 **The personal data we <u>will</u> collect will be used for the following purposes:**

- To assist you with income tax compliance and tax advise

3.6 **The personal data we <u>may</u> collect could be used for the following purposes:**

- **<u>In relation to the Customer</u>**

  Personal information relating to your appropriateness for the job and to enable the working relationship between yourself and the customer.

- **<u>In relation to third party providers to the Customer</u>**

  In some instances your personal information may be shared with other sub-contractors that the customer needs to contract with to complete the work.

- **<u>Local Agent Initiation services</u>**

  In some countries of deployment it is mandatory that you are employed in that state or country. In such cases a local agent will be used to facilitate this requirement.

  This could include (but is not limited to) the provision of the following;

  - The securing of Visas, residency, work permits and relevant employment contracts. This could include (but is not limited to)

  - In country medical insurance.
  - Qualification documentation to verify your educational status
  - Information about your dependents or relatives.
- The setting up of a place of residency in the country of deployment for you. This could include (but is not limited to)
  - Information relating to utility services provided to that place of residence
  - Information relating to the provisioning of driving license requirements.
- The establishment of a method to pay you by, typically the setting up of a bank account in the country of deployment.

- **In relation to your health and welfare**

  In some countries it will be necessary to provide you with Health Insurance & Health care

- **In relation to the attestation of certificates and legal documentation**

  In some cases it will be necessary to use the services of a company to attest to the vailidity of some of the documents you will be required to provide in relation to your deployment.

- **Place of Employment security clearances**

  Information relating to verification of your security appropriateness to work on the site you have been deployed to. This would include all information required to carry out security and pre-vetting checks.

- **In relation to Legal cases that may arise in countries of deployment**

  On rare occasions we may use your personal data in defence of a legal case in the country of secondment.

3.7 Legal Basis for processing your data

Our legal basis for processing your data in relation to tax advise and guidance is: LEGAL OBLIGATION in compliance with financial law.

We are legally obliged to provide a duty of care to you whilst you are on deployment. In such cases where Health Insurance & Health care is necessary our legal basis for doing this is LEGAL OBLIGATION.

Our legal basis for processing the data that we *may* collect is LEGITIMATE BUSINESS INTEREST.

However if we are transferring your data to a country that is considered by the Eurpoean Union to have inadequate data protection laws in place we will use CONSENT from yourself as the Legal

basis for processing under Article 49 of the GDPR to transfer data to a country with inadequate data protection laws.

If the data is classed as special category, and we are transferring your data to a country that is considered by the Eurpoean Union to have inadequate data protection laws in place we will use EXPLICIT CONSENT from yourself to transfer the data.

In such cases we will enter into a consent agreement with you which will fully outline what data will be processed, why and the risks that your data could be subject to and what security provisions the Company is able (and has put in place) to protect your data.

On the rare occasion when your data was used in defence of a legal case the legal basis of processing would be variable depending on what type of case it is. In all such cases we would inform you of our intention to process the data and our reasons for doing so.

3.8 If you give us someone else's personal data

Sometimes you might provide us with another person's personal data – e.g. because they will be accompanying you or they are an emergency contact or next of kin.
In such cases, we require you to inform the individual what personal data of theirs you are giving to us. You must also give them our contact details and let them know that they should contact us if they have any queries or concerns about how we will use their personal data. Please provide them with a copy of this privacy notice, so that they are aware of theirs rights and how they can exercise them.

3.9 Disclosure

Your information could be shared internally, including with members of the HR and, Payroll, your line manager, managers in the business area in which you work, the risk management team and IT staff if access to the data is necessary in the performance of their role.

We could share your data with the following third parties:

- A country's government
- A country's government's licensed agency.
- An in country local agent to facilitate residency, employment etc. in the deploying country.
- Estate Agents
- Utilities Companies in relation to your place of residence
- Your countries embassy or consulate
- A third party Service or product provider
- Residency maintenance services
- External tax advisors

We share your data with third parties in order to:

- Pay you

- Ensure that you comply with the host country's rules and regulations.
- Providing you with appropriate accommodation and services
- Facilitate yours and/or your dependents travel requirements.
- To provide you with tax advise and ensure that you continue to comply with your country of permanent residency tax laws during your period of deployment.
- To protect the legal interests of the Company and potentially (but not in all cases) yourself.

All Travel requirements will be provided by the Company Travel Service provider. All travel **MUST** be booked via the Travel Service Provider, see your primary Privacy Notice for full details.

3.10 **Transferring personal data to other countries**

All Countries within the European Union are covered by the GDPR, so your personal data will be handled and managed in exactly the same way as you would expect in other EU Countries and can therefore be transferred without any other additional controls in place.

Other Countries considered to have adequate Data Protection laws in place are the additional countries included in the European Economic Area (Norway, Iceland & Liechtenstein) and the countries identified in following link:- https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

In all other Countries where your personal data may be transferred the Company will ensure that appropriate measures are in place to protect it and will inform you of the transfer of data and the reasons why it is necessary. We will also request your consent to do so, if a binding agreement or an alternate agreement can not be put in place to confirm the security of your personal information.

Retention period

Where we can guarantee the management of your personal data it will be held for the duration of the deployment or longer if there is an overriding legal requirement for it to be so.

Where we cannot guarantee by law that your personal data will be deleted we will take all measures possible to request that it is, as soon as Visa requirements and/or your deployment is at an end or you have withdrawn your consent for processing.

All UK and EU organisations involved in the project will meet the GDPR requirements by law.

3.11 **Your rights as a data subject**

At any point while we are in possession of or processing your personal data, you, the data subject, have the following rights:

- Right of access – you have the right to request a copy of the information that we hold about you.
- Right of rectification – you have a right to ask for data that we hold about you that is inaccurate or incomplete to be corrected.
- Right to be forgotten – in certain circumstances you can ask for the data we hold about you to be erased from our records. If there is no overriding legal reason to keep it.
- Right to restriction of processing – where certain conditions apply to have a right to restrict the processing.
- Right of portability – you have the right to have the data we hold about you transferred to another organisation.
- Right to object – you have the right to object to certain types of processing
- Right to object to automated processing, including profiling – You have the right to ask for certain important computer-made decisions (including profiling) to be challenged and to ask for a human to intervene.
  (Please note that at this time no automated processing of Personal Identifiable Information (PII) is in operation.
- in the event that Marshall refuses your request under rights of access, we will provide you with a reason as to why.
- Where the legal basis for the processing of PII data is 'consent', you have the right to withdraw that consent at any time and the record will be deleted where there is no overriding legal basis to keep it.
  Please note that it is the company's policy not to use consent for the legal basis for process except in exception cases with the express approval of the Data Privacy Manager
  You have the right to complain as outlined in clause 3.10 below.
-

All of your rights identified above apply to any third party (as stated in 3.5 and 3.6 above) should they be involved in the processing of your personal data.

If you would like to exercise any of these rights, please contact the company Data Privacy Manager, by emailing DataPrivacyManager@MarshallADG.com or by sending written correspondence to The Data Privacy Manager, Marshall, Airport House, Newmarket Rd, Cambridge, CB5 8RX.

You can make a subject access request by completing the organisation's Subject Access Request Form

3.12 **Complaints**

In the event that you wish to make a complaint about how your personal data is being processed by Marshall (or third parties as described in 3.6 above), or how your complaint has been handled, you have the right to lodge a complaint directly with

Marshall's Data Privacy Manager, by emailing DataPrivacyManager@MarshallADG.com or by sending written correspondence to The Data Privacy Manager, using the contact details below.

If the complaint is not resolved to your satisfaction you have the right to lodge the complaint with the Supervisory Authority.

The details for each of these contacts are:

	Data Privacy Manager	**Supervisory Authority**
Contact Name:	Isobel Aylott	Information Commissioners Office (ICO)
Address line:	Marshall, Airport House, Newmarket Rd, Cambridge, CB5 8RX	Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF
Email:	DataPrivacyManager@MarshallADG.com	https://ico.org.uk/global/contact-us/email/
Telephone:	01223 373206	03031231113
Website		https://ico.org.uk/concerns/

The recommended method of communication to the ICO is via their website

Document Owner and Approval

The Data Privacy Manager is the owner of this document and is responsible for ensuring that this record is reviewed in line with the review requirements of the GDPR.

A current version of this document is available to all members of staff on the Company Internet

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	New release of a Privacy Notice dedicated to staff who are being seconded under Global mobility, separating it out from primary privacy notices to make it easier for Data Subjects to understand the requirements etc.	Isobel Aylott	10/09/2020
2	Removal of Marshall ADG as the overarching definition of the group of companies	Isobel Aylott	08/09/21

APPENDIX A– FURTHER DETAILS

This section of the Secondee Privacy Notice tells you in more detail about the type of personal data we WILL hold about you, what we use it for, our legal grounds for doing so, who we share it with and how long we keep it.
Where we process additional Personal data specifically relating to the deployment you have been seconded to which requires your explicit consent this will be covered in the consent agreement.

Note also that the first two Tables below divide items of personal data into relatively broad categories (under the heading "Type of ordinary personal data held by us", or "Type of special category personal data held by us"). Where multiple purposes and/or legal grounds for our use of a given "type" of personal data are identified, this does not necessarily mean that *all* of the purposes and/or legal grounds are applicable to *all* items of personal data falling within that "type" of personal data.

More information about your ordinary personal data

Type of ordinary personal data held by us	What we use it for	Legal ground
Surname, First Name, Middle Name, Job Title, address, Salary and other renumerations and benefits.	Provide yourself with income tax advice and submitting any legally required data to HMRC (or your originating country of employment) to ensure you comply with their tax laws.	Legal obligation Under duty of care and financial law.

More information about your special category data

Type of special category data held by us	What we use it for	Legal ground	Special category legal ground
At this time all special category data involved in deployments requires explicit consent and is covered by Consent Agreements.			

More information about how we share your personal data

Who we share your personal data with	What data we share	Why we share it	Legal ground
Marshall Group	Insurance Information	To ensure you are appropriately insured to cover your deployement.	Legal obligation