Guide to the General Data Protection Regulation

2nd Edition - 2020

Contents

Introduction

The GDPR is an EU Regulation which sets out how all organisations, large and small, are required to handle personal data. Its core concept is that the privacy of individuals must be respected and protected. One consequence of this protection is that a range of obligations are placed on all businesses which handle personal data, with potential penalties for organisations which do not comply with these obligations.

The GDPR is highly relevant to EuRA members. As a relocation business, you obtain personal data from your clients in order to deliver personalised services. The data are likely to be shared, stored, amended and, finally, deleted by you. Whatever the exact form of "data processing" which takes place, it is important that you are compliant with the GDPR.

The purpose of this Guide is to explain the main practical implications of the GDPR for EuRA members. We also provide links to more detailed guidance provided by national data protection authorities (Chapter 12) and an example of a company's Privacy Standard (see Appendix).

Compliance with data protection rules is the responsibility of everyone in your business, so the need for staff training and supply-chain communication should not be underestimated. While the rules can seem burdensome, the real prize is to build GDPR-compliant processes which help to make your business more efficient and fully aligned with the needs of clients.

Finally, we have to emphasise that the purpose of this Guide is to provide EuRA members with a helpful overview of the GDPR and is not intended as a substitute for professional advice.

Gordon Kerr
EuRA Strategic Consultant - Legal Services

May 2020

1. The GDPR: a quick overview

With effect from 25th May 2018, the GDPR introduces a single legal framework across the EU for handling personal data. Many of the core principles and obligations contained in the old law (from 1995) remain unchanged, but the GDPR also imposes some new and additional requirements.

There are now **six principles** which govern the processing of personal data:-

1. **Lawfulness, fairness and transparency**.
2. **Purpose limitation** - you only collect and process personal data for "specified, explicit and legitimate" purposes.
3. **Data minimisation** - you collect only data which is "relevant" and is "limited to what is necessary".
4. **Accuracy** - all data held by you is accurate and up-to-date.
5. **Storage limitation** - you do not retain personal data for longer than is necessary to fulfil the purposes for which the data was collected.
6. **Integrity and confidentiality** - your business has appropriate data security measures in place.

Your business needs to comply with these six principles and also be able to demonstrate compliance. This requirement to demonstrate compliance is called "**accountability**" and is a key element of the GDPR.

Data Protection Authorities (DPAs) across the EU have stressed that the GDPR should not be seen as a revolutionary change, but describe it instead as an "evolution" of current law, updated to reflect the enormous changes which have taken place in how we all use technology (and share data) on a day to day basis.

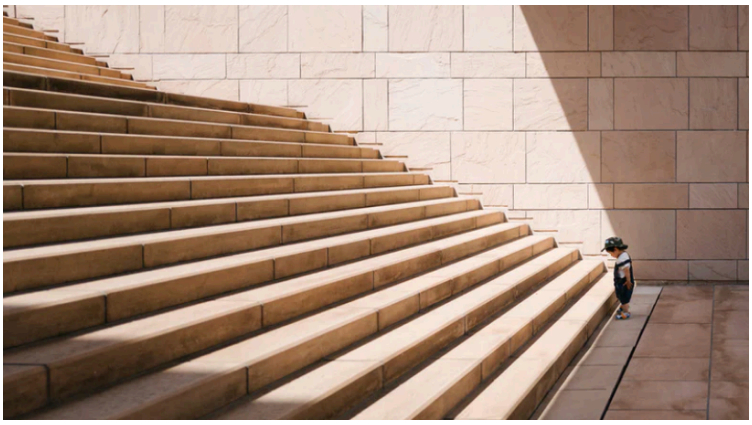
So what did the GDPR actually change?

- One data protection law across all EU and EEA countries
- Application of law outside the EU (businesses will be subject to the GDPR if they target EU consumers, even if the businesses are not established in the EU)
- Higher fines (*up to 4 percent of yearly worldwide revenues or €20 million, whichever is greater*)
- Tighter rules on "consent" to personal data use
- "Privacy by Design" and "Privacy by Default" (*service processes require to be designed from the outset to ensure an adequate level of privacy for an individual's personal data*)
- *Stricter rules on reporting security breaches*
- New obligations on how access enquiries from individuals must be handled

In the sections below, we explore what the GDPR means, in practical terms, for relocation businesses.

2. Your GDPR starting point: a data audit

Before going any further, it is important to understand an important distinction made under data protection law: that between "data controller" and "data processor". This can get complicated but understanding whether you are acting as a controller or processor is important.



The controller is the business which determines the purpose for which – and the way in which – personal data is processed. It is the controller which has primary responsibility for ensuring that the law is being fully complied with and faces potential penalties if things go wrong. The processor is the business which processes personal data on behalf of a controller. The processor must also comply with the law, but its legal obligations are secondary to those of the controller.

In practical terms, in the relocation industry, this controller/processor distinction means that:

- An employer is controller of the data which it holds on its own employees;
- A relocation management company (RMC) will usually be a processor, but this can be varied by the terms of the employer/RMC contract and it is not uncommon to find that both employer and RMC are acting as controllers;
- A destination services provider (DSP) instructed by either an employer or an RMC is a processor; but if a DSP contracts direct with an individual then, in that situation only, the DSP is a controller
- All relocation businesses are controllers of the personal data held on their own employees.

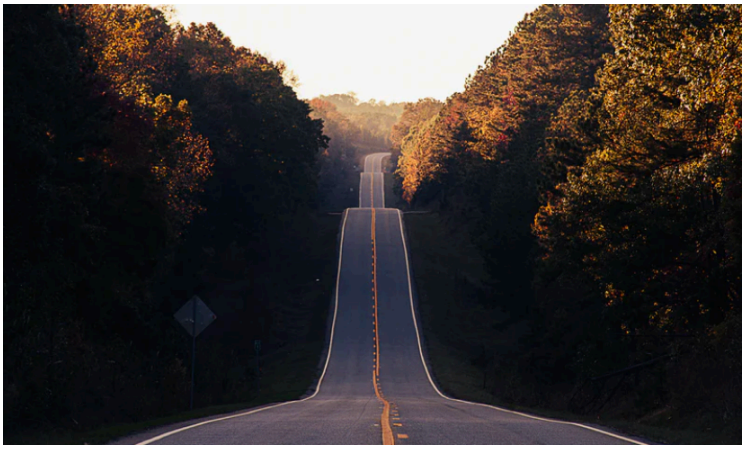
In order to comply with the GDPR, it is important that you have a clear picture of the current flows of personal data within your business and exactly how and why you process the data. Note that processing includes any interaction with personal data, e.g. collecting, storing, using, altering or deleting; while "personal data" is any information that can identify a living individual.

A good starting point is to answer the following questions:

- Whose data do you process? e.g. your individual customers and their families, individual corporate contacts, your employees, business development targets and any other 3rd party data (individuals, not businesses)
- Is any "sensitive" data included? this is referred to in the GDPR as "special categories" and includes personal data relating to health, religion, sexual orientation, political affiliations or genetic or biometric data
- How do you obtain personal data? e.g. direct from individuals and/or from corporate clients and RMCs
- What do you do with data? e.g. used only for delivering authorised relocation services, maintaining employee records and not used for marketing purposes
- Why do you do these things? e.g. a necessary part of delivering agreed relocation services, complying with employment law and good employment practices
- Where do you store data? - and for how long?

- Is all stored data up-to-date, accurate and relevant?
- Do you share personal data with any 3rd parties? e.g. with partners or sub-contractors
- Do you ever transfer data outside the EU?

Based on the information you have collected by answering these questions, you can now delve into what your business needs to do to comply fully with the GDPR.



3. Understanding the "lawful basis" of your data processing

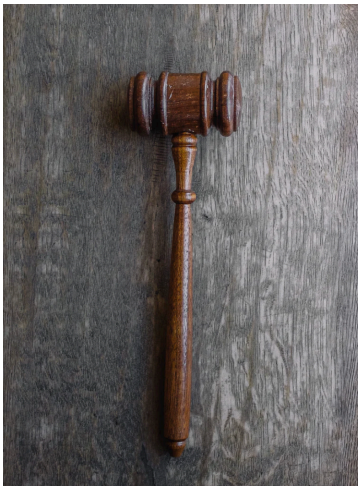
You need to be clear about the legal basis for each form of data processing which you carry out in the course of delivering services to clients. The GDPR sets out six different "lawful bases of processing", but most relocation businesses will rely on just four of these:

a. Consent of the individual, or

b. Performance of a contract, or

c. Legitimate interest, or

d. Legal obligation



a. Consent

It is important to be clear about exactly what we mean by "consent" here. Consent is defined in Article 4(11) of the GDPR as:

"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

Many relocation businesses make use of consent clauses or ask customers to sign stand-alone consent forms. The wording should now be carefully checked to ensure that it complies with the definition above. If it does not, then the document wording should be updated.

You need to be particularly careful if your relocation service includes the processing of sensitive data, such as health information. This is referred to in the GDPR as "special categories" of data and requires explicit consent to processing. Explicit consent is also required for cross-border data transfers.

b. Contractual obligation

Your business does not need to rely on consent when the processing is necessary for performing a contract with the customer. So, where you are simply gathering minimum data (e.g. name and contact details) in order to deliver a relocation service ordered by the customer, you do not also need the customer's specific consent to process that data.

The processing must be necessary in order to deliver the contracted services. If you could reasonably do what your customer has requested without processing their personal data, the contract will not be a lawful basis for processing the data.

The contract does not have to be a formal signed document, or even written down, as long as there is an agreement which meets the requirements of contract law. But the contract must be with the individual whose personal data is being processed. It is not a lawful basis if you process an individual's details but the contract is with someone else.

The processing must be necessary in order to deliver your contractual obligations to the individual customer. If the processing is only necessary because it is helpful to your business in a wider sense, the contractual lawful basis will not apply and you will need to consider another lawful basis, such as legitimate interest.

c. Legitimate interest

Legitimate interest is the most flexible lawful basis for processing personal data. It is appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact.

If your business chooses to rely on legitimate interests, bear in mind that you are taking on some additional responsibility for considering and protecting your customers' interests.

There are three elements to the legitimate interest basis. You need to:

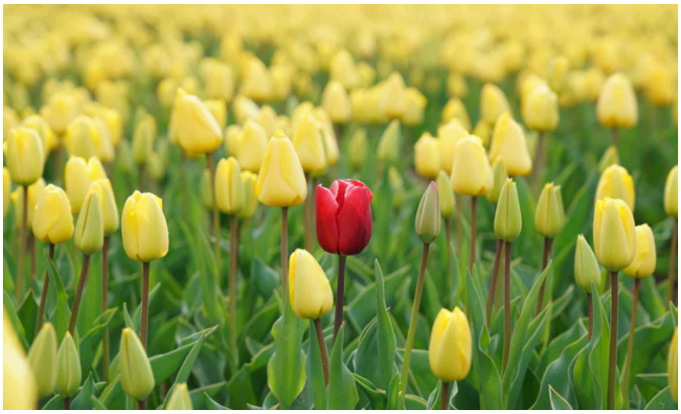
- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.

It seems likely that relocation businesses will prefer to rely on specific consents from individual assignees.

d. Legal obligation

In addition to customer data, it is likely that you also process personal data of your employees. The lawful basis for this will normally be a combination of your contractual obligations (under each employment contract) and the lawful basis of "legal obligation". This latter basis would include the requirement of your business to disclose employee salary details to your national tax authority, for example.

You should include details of your lawful basis for processing your customer's personal data in your privacy notice (see next section).



4. Your responsibilities to individuals

The GDPR made some enhancements to the rights which individuals have in relation to their personal data. The rights which are of most relevance to a relocation business are:

- **the right to be informed** - you need to provide certain information, usually done through a privacy notice, such as your business identity and how you intend to use the data. You also need to advise if the data will be shared or transferred outside the EU. The GDPR added some further obligations to this list, including:
    - your " lawful basis" for processing the data (see above)
    - your data retention periods
    - individual's right to complain to your national data protection authority
    - - all provided in concise, easy to understand and clear language.

- **the right of access** - individuals are entitled to know exactly what personal data your business is holding

- **the right to rectification** - any inaccuracies reported to you in the data held by you must be rectified

- **the right to erasure (to be forgotten)** - note that this does not apply while you are processing data as part of your contractual obligation

Each of these rights provides individuals with a level of control over personal data which is held by your company. To ensure that you are meeting your obligations in respect of these individual rights, you should review:

- your privacy policies and consent forms
- your procedures for seeking and recording consent - and also for recording any withdrawals of consent
- your procedures for handling requests from individuals, e.g.
    - can you locate relevant data within the required timescale (now reduced from forty days to one month)?
    -
    - are you sure that all requests for data corrections will be acted upon?
    - should you consider introducing systems which allow individuals to access their information online?

<u>Updating Privacy Notices</u>

The GDPR places a strong emphasis on the need to be completely transparent. More information must be contained in a privacy notice and businesses are obliged to use clear language and to ensure that the notice is readily accessible.

Your privacy notice should include:

- the name of your organisation and a contact
- purpose and legal basis of data processing
- categories of data processed
- any parties with whom you will share data
- details of any international transfers of data and relative safeguards
- the existence of individual rights, including the right to withdraw consent (if relying on consent) and the right to complain to a data protection authority.

5. Retaining data

All personal data held by your business should be limited to what is necessary to enable you to deliver the particular services which your client has authorised. In particular, you cannot collect information just because you find it interesting or may have a use for it in the future.

Personal data should not be retained by your business for longer than is necessary. Your data retention policy should, however, take into account your ongoing reporting obligations, including any necessity to retain individual records for the purposes of future reporting to tax authorities.

Sometimes there will be minimum and maximum retention periods specified in legislation. For example, the UK's 2017 Money Laundering Regulations specify that relevant documents and information must be retained for a minimum of five years and a maximum of ten years, unless the client has given consent to a longer retention period.

But, more commonly, businesses have to make their own judgement calls about data retention periods. So, consider what you think is reasonable for the different types of service which you deliver and be prepared to justify your decisions.

Once you have reviewed your data retention policies, it is important to ensure that personal information is *actually* being deleted in accordance with your updated policies.

6. Data security and handling a data breach

Your business is required to take "appropriate technical and organisational measures" to secure personal data. When addressing privacy protecting measures such as staff training or encryption, for example, you are able to consider the cost of implementation, available technology and the level of risk and context of the processing. This means that a degree of proportionality can be applied.

But, whatever security measures you have in place, there is always a risk of data breaches. The GDPR introduces compulsory reporting of *some* data breaches to your data protection authority and in some cases you may also be required to notify affected individuals.

Incidents which must be reported to your DPA include not only the loss or disclosure of personal data, but also where there has been destruction of data or unauthorised access. However, there is a risk-based approach to reporting where an incident is "unlikely to result in a risk to the rights and freedoms" of any individuals. The timescale for reporting an incident to your DPA is 72 hours.

In addition to the report to your DPA, your business will also have to report the incident to affected individuals if it is likely to result in a high risk to the rights and freedoms of those individuals. This obligation is not absolute and in some cases, such as where the data was properly encrypted, they will not have to be informed.

There is also an obligation on data processors (e.g. a DSP) to notify their controller (e.g. a corporate client) "without undue delay" after becoming aware of a breach.

7. Reviewing your contracts

The GDPR makes written contracts between controllers (e.g. a corporate client) and processors (e.g. a DSP) a requirement. These contracts must now include certain specific terms. Similarly, if a processor employs another processor (e.g. a local sub-contractor), it also needs to have a written contract in place.

The GDPR gives processors responsibilities and liabilities in their own right, and processors as well as controllers may now be liable to pay damages or fines. The intention behind the new, stricter rules is that controllers and processors will have a clearer understanding of their respective obligations and responsibilities.

Contracts must set out the content and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller. Every contract must also require the processor to:

- only act on the written instructions of the controller;
- ensure that employees (and others) processing the data are subject to a duty of confidence;
- take appropriate security measures;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing "subject access" and allowing individuals to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their GDPR obligations, and tell the controller immediately if it is asked to do something infringing data protection law.

In addition to these contractual obligations, a processor now also has its own direct GDPR responsibilities, including:-

- not to use a sub-processor without the prior written authorisation of the data controller;
- to co-operate with data protection authorities (such as ICO in the UK, CNIL in France, etc);
- to ensure the security of its processing;
- to notify any personal data breaches to the data controller.

If a processor fails to meet any of its GDPR obligations, or acts outside the instructions of the controller, then it may be liable to pay damages or be subject to fines. In addition, if a processor uses a sub-processor, it remains directly liable to the controller for the performance of the sub-processor's obligations.

Finally, be aware that if the reality is that a processor "determines the purpose and means of processing" (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.

8. Transferring data to other countries

The EU has always imposed strict rules on transfers of personal data to countries outside the EU. These rules remain largely unchanged although there are some additions to the restrictions in place.

"Consent" continues to be a valid basis for international transfers, but this is the new more rigorous test for consent imposed by the GDPR, which means that individuals must be provided with very clear communication on where your business will be sending their data (outside the EU) and how their data will be protected.

A starting point is to check the EU's **approved list of countries** which provide "adequate protection" of personal data. At this time, only Switzerland, Guernsey, Argentina, Isle of Man, Faroe Islands, Jersey, Andorra, Israel, New Zealand and Uruguay have been approved in full. Canada and Japan have been approved for certain types of personal data. But, for example, Australian privacy law is not, currently, considered to provide an adequate level of protection for personal data from the EU.

This means that, personal data transfers from EU countries, to countries such as Australia, must be protected by one of the specific methods approved by the EU Commission. Currently, these are:-

- for **internal data transfers** (if your company is part of an international group) - implement corporate rules for transferring data, in the form of EU-approved ***Binding Corporate Rules***;

- for **3rd party data transfers** - incorporate EU-approved ***Standard*** (or ***Model***) ***Contract Clauses*** in all contracts with non-EU 3rd parties which make reference to the transfer of personal data;

- for **data transfers to the United States** - ensure that the US organisation receiving the data is registered under the **EU-US Privacy Shield.** This is the certification which replaced "Safe Harbour" in 2016 and most RMCs have obtained accreditation. A similar Privacy Shield exists for personal data transfers from Switzerland to the United States.

The GDPR outlines the factors which the European Commission will consider when determining whether a non-EU country meets the necessary standards for safe transfers to take place. To be found "adequate", a country must have a data protection regime "essentially equivalent" to the GDPR. This is why, post-Brexit, UK data protection law will continue to incorporate the GDPR.

Unlike previous data protection law, the GDPR now restricts not only the first transfer of personal data from Europe to a third country but also any onward transfer of data from that territory. EU relocation companies should review carefully all contracts which cover international transfers of personal data.

9. Privacy Rights of your own Employees

In focusing on the protection of personal data held on your customers, there is a danger of overlooking the obligations to protect the information which you hold on your own employees and to respect their privacy rights.

Businesses generally hold personal data for prospective, current and former employees. This may include contact details, CVs, employment contracts, employment records, performance reviews, complaint files, benefits, references, meeting minutes, emails and bank details. So, the starting point, for GDPR compliance purposes, is to determine what employee data your business currently holds and in what format (paper and/or electronic).

Having worked out the types of data held in your HR records, you then need to be clear about your lawful basis for collecting and retaining these various categories of data. In practice, this will be a combination of your obligations under each employment contract, your general legal obligations (to maintain tax records, for example) and the broad GDPR category of "legitimate interest of your business." Your business should have processes in place for ensuring the security of data, its accuracy and its deletion when no longer legitimately required.

Under the GDPR, your employees are entitled to more information about how their data is processed. This is usually done in the form of a Privacy Notice. If relevant, your business should also issue policies on employee monitoring, bring-your-own-device or remote working, acceptable Internet and email use and reporting data requests and data breaches. You also need to be aware of the enhanced rights of your employees in relation to "access" (i.e. to know exactly what data is held on them), right to object to processing, right of rectification (i.e. if any data is inaccurate) and right to be forgotten.

10. How RMCs are implementing the GDPR

Many aspects of the GDPR call for some interpretation and judgement calls. This means that there is no single GDPR implementation model for the diverse range of RMCs which operate in the global marketplace. However, there are common approaches in some areas:-

- **changes to internal processes**

To accommodate the expanded definition of personal data, RMCs are revising their various internal policies, their external privacy policies and their data handling practices.

Data retention policies are being reviewed and updated to ensure that data is not being retained for longer than needed, taking into account not only the GDPR, but also applicable laws and client audit requirements. Where back-up functions cannot easily segregate and apply different rules to EU data and non-EU data, new technical measures are being introduced to provide for either on-line archiving systems with a purge of personal data elements, or the "pseudonymization" of personal data.

Increasingly, assignees are able to access and rectify their data held on RMCs' online systems. At the same time, online privacy statements and consent forms are being updated to provide individuals with clear explanations on exactly what data is collected, how it is used and with whom it is shared.

- **changes to contracts with suppliers**

Many RMCs are working with their supplier networks to augment existing Data Transfer Agreements (DTAs), which are "onward transfer" agreements that allow an RMC to legally transfer personal data originating in EU countries to its suppliers. DTAs allow the supply chain to operate in accordance with current data protection law, including the Model Contract Clauses and Privacy Shield frameworks. In preparation for the GDPR, DTAs are now being augmented by Data Protection Amendments, which update the underlying data privacy provisions in existing supplier agreements.

- **changes to contracts with clients**

Some contract changes are being introduced to take account of the stronger requirements relating to "consent" and how appropriate consents should be obtained from assignees. More generally, RMCs are having to respond to a range of proposed revisions which their corporate clients are deeming to be prudent.

- **appointment of Data Protection Officers (DPOs)**

Many RMCs have appointed DPO's.

The legal requirement for a relocation company to appoint a DPO only arises if its "core activities" involve processing operations which require regular and systematic monitoring of data subjects on a large scale. However, even if a DPO appointment is not mandatory, the data protection authorities encourage voluntary designation of a DPO.

Several RMCs have appointed voluntary DPOs to help guide compliance with data protection laws and to be available for inquiries from individuals and from data protection authorities. The DPO can be an individual or a DPO team.

- **training and audits**

Many RMCs are planning additional data protection training for suppliers and it is likely that suppliers will be subject to more regular and/or stringent audit checks. Ultimately, RMCs will be unable to conduct business with suppliers which cannot adhere to the requirements of the GDPR.

- **breach reporting**

RMCs updated their security incident response processes and tracking. Staff training on data protection was stepped up, including the need to report incidents.

- **reviewing if RMC is operating as "controller" or "processor"**

This can be a surprisingly difficult issue. The starting point is that a controller controls the purposes and means of using personal data, while a processor processes data on behalf of the controller. One view is that the corporate client is the controller and the RMC and its supply chain are all processors. But it is possible for an entity to be both a controller and a processor and that can be the case when the RMC is delivering its guaranteed homesale service, for example.

An alternative view is that, where relocation support is fully outsourced by the corporate client to an RMC, both the client and the RMC are controllers.

Whatever the legal view taken by an RMC, the important point is that their service contracts should contain data protection clauses which include clarity around where the controller/processor responsibilities lie. The GDPR means that there is now greater responsibility on those drafting Relocation Service Agreements (e.g. in-house lawyers at RMCs and at their corporate clients) to understand the personal data flows which occur and the GDPR consequences of these data flows.

11. Frequently Asked Questions

Here are a few practical questions which come up regularly in discussions about the GDPR:-

1) Does the GDPR mean that data protection laws are now identical in all EU countries?

A main purpose of the GDPR is to strengthen and unify data protection law within the EU. However, the harmonisation of laws will not be achieved completely because of the so-called "opening clauses". The opening clauses cover a wide variety of aspects relating to data protection.

For example, countries are allowed to implement national rules on issues, such as the requirements for the designation of a data protection officer, the age of consent of children, data protection in the context of employment and data breach notification obligations.

There will continue, therefore, to be some national variations in data protection laws, but it seems unlikely that these variations will have much practical impact on the steps being taken by relocation businesses to comply with the GDPR.

2) Does Brexit mean that the GDPR will not apply to the UK?

No - the GDPR will continue to apply to the UK for the foreseeable future. The UK's Data Protection Bill will shortly repeal and replace the Data Protection Act 1998. When the UK leaves the EU, the Bill allows for the continued application of GDPR standards and the GDPR will be incorporated into UK domestic law.

So, the plan is that the UK and EU data protection regimes will continue to be aligned, which allows the UK to become an "adequate jurisdiction" for EU data and have uninterrupted data flows once the UK has left the EU.

3) Will large fines be imposed for GDPR breaches?

There has been a lot of scaremongering on this issue, probably due to the huge increases in the maximum fines which DPAs can impose under the GDPR. But the statements actually issued in recent months, by the DPAs, focus very much on "carrot" rather than "stick". They talk about an overriding "commitment to guiding, advising and educating organisations about how to comply with the law." It is also worth highlighting that last year 17,300 cases were concluded by the UK's DPA (ICO) and that only 16 of these cases resulted in fines.

It is important to get to grips with your GDPR obligations, but beware expensive consultants offering to save your business from imminent financial ruin!

4) Do we need to appoint a Data Protection Officer (DPO)?

It is unlikely that any relocation business would require to appoint a DPO, though some may decide to go down this route voluntarily. Under the GDPR, a DPO requires to be appointed by a company in the following circumstances:-

- the organisation is a public authority, or
- the company's core activities consist of systematic monitoring on a large scale, or
- the company's core activities consist of processing on a large scale of sensitive personal data.

If your business is not appointing a DPO, you may want to consider nominating an employee (or an external consultant) who will have overall responsibility for data protection matters.

5) Does the GDPR affect our use of "cloud" services?

With reference to cloud computing, the short answer is that the GDPR is neutral, i.e. it neither prevents nor recommends the use of the cloud.

Instead, there is an overriding obligation on your business to ensure the security of personal data and the appropriate level of security will depend on a number of factors including the technology solutions available, costs of implementation and the types of data processing activities undertaken. All businesses are expected to weigh the affordability of cloud storage against the increased possibility of hacking, bearing in mind the potential impact on the individuals who could be affected. However, there is certainly no suggestion that cloud services such as Microsoft 365 are unsuitable for relocation management purposes.

6) If we breach the GDPR, can we be sued for damages by individual "data subjects"?

Yes. A GDPR breach can give rise to a claim for damages against the offending company if an individual affected by the breach can show either financial loss or "distress" (e.g. embarrassment at private details being made public). The right of an individual to sue for compensation has always existed (i.e. long before the GDPR came into force), but it's likely that we will a rise in private claims as members of the public now have greater awareness of their privacy rights. A group of individuals affected by the same data breach can also sue for damages as a group, in what is called a "class action".

12. Sources of Further Information

Further information on how to comply with the GDPR is available on the following websites of the national data protection authorities of each EU country:-

- Austria: http://www.dsb.gv.at
- Belgium: http://www.privacycommission.be/
- Bulgaria: http://www.cpdp.bg/
- Croatia: http://www.azop.hr/
- Cyprus: http://www.dataprotection.gov.cy
- Czech Republic: https://www.uoou.cz/
- Denmark: http://www.datatilsynet.dk
- Estonia: http://www.aki.ee/en
- Finland: http://www.tietosuoja.fi/en/
- France: http://www.cnil.fr/
- Germany: http://www.bfdi.bund.de/
- Greece: http://www.dpa.gr/
- Hungary: http://www.naih.hu/
- Ireland: http://www.dataprotection.ie/
- Italy: http://www.garanteprivacy.it/
- Latvia: http://www.dvi.gov.lv/
- Lithuania: http://www.ada.lt/
- Luxembourg: http://www.cnpd.lu/
- Malta: http://www.dataprotection.gov.mt/
- Netherlands: https://autoriteitpersoonsgegevens.nl/nl
- Poland: http://www.giodo.gov.pl/
- Portugal: http://www.cnpd.pt/
- Romania: http://www.dataprotection.ro/
- Slovakia: http://www.dataprotection.gov.sk/
- Slovenia: https://www.ip-rs.si/
- Spain: https://www.agpd.es/
- Sweden: http://www.datainspektionen.se/
- United Kingdom: https://ico.org.uk

The European Commission has produced various guides to the GDPR. The most recent overview, with guidance for small and medium-size businesses can be found at http://ec.europa.eu/justice/smedataprotect/index_en.htm.

13. Glossary of Terms

Cloud computing - Internet-based computing, where different services — such as servers, storage and applications — are delivered to an organisation's computers and devices through the Internet. The cloud infrastructure is maintained by the cloud provider, not the individual cloud customer.

Data Controller - the person or business which determines the purposes for which, and the way in which, personal data is processed.

Data Processor - a business which processes personal data on behalf of a data controller

Data Protection Authority (DPA) - a country's data protection supervising authority

Data subject - the person about whom personal data is being collected, processed and stored.

EU-US Privacy Shield - a certification, approved by the European Commission and the US Department of Commerce, which enables companies to make transfers of personal data from the EU to the US

Information Commissioner's Office (ICO) - the data protection authority for the UK

Personal data - data relating to a living individual who can be identified from the data, including e.g. contact details, photograph, correspondence and biometric data (see also "*sensitive personal data*")

Processing (of data) - any interaction with personal data, including collecting, storing, using, altering and deleting

Pseudonymization (of data) - a procedure by which the most identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms

Sensitive personal data - data which could be used in a discriminatory way and is likely to be of a private nature, so needs to be treated with greater care than other personal data. This includes information on racial/ ethnic origin, religion, political activities, sexual life and health issues. (*see also "personal data")*

***Appendix** - Example of a Privacy Standard*

*[**insert COMPANY NAME**] - **Privacy Standard***
(an outline for employees of how the Company complies with the GDPR)

1. EXPLANATION OF LEGAL TERMS USED IN THIS PRIVACY STANDARD

***Consent:** the Data Subject's agreement to the Processing of Personal Data relating to them, by a statement or by a clear positive action. Consent must be freely given, specific and informed.*
***Data Controller:** we act as Controller when we are determining the purpose for which, and the way in which, personal data is processed. For example, we are Controller in relation to the Personal Data which we hold on our employees. The Controller has primary responsibility for ensuring compliance with the GDPR.*
***Data Processor:** we act as Processor when we process personal data on behalf of a Controller. For example, we will normally be a Processor when we are acting as a service provider to relocation management company. The Processor must comply with the GDPR, but its legal obligations are secondary to those of the Controller.*
***Data Subject:** a living, identified or identifiable individual about whom we hold Personal Data.*
***EEA:** the 27 countries in the EU, and Iceland, Liechtenstein and Norway.*
***General Data Protection Regulation (GDPR):** the EU's Regulation imposing strict legal safeguards in relation to Personal Data.*
***Personal Data:** any information identifying a Data Subject or information relating to a Data Subject that we can identify. 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 Breach:** any act or omission that compromises the security or confidentiality of Personal Data or the safeguards that we or our third-party service providers have put in place to protect it. The loss or unauthorised access of Personal Data is a Personal Data Breach.*
***Privacy Notices or Privacy Policies:** notices setting out privacy information for Data Subjects to be used when the Company is acting as Data Controller.*
***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 or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.*
***Related Policies:** the Company's policies, operating procedures or processes related to this Privacy Standard and designed to protect Personal Data. See Appendix.*
***Special Categories of Personal Data (**also called **"Sensitive 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.*

2. INTRODUCTION

This Privacy Standard sets out how we handle the Personal Data of our customers, suppliers, employees and other third parties. It applies to all Personal Data we Process regardless of the media on which that data is stored.
This Privacy Standard applies to all Company personnel. You must read, understand and comply with this Privacy Standard when Processing Personal Data on our behalf and attend training on its requirements. This Privacy Standard sets out what we expect from you to ensure that the Company complies with the GDPR and other applicable laws. Your compliance with this Privacy Standard is mandatory. Related Policies, referred to in the attached Appendix, are available to help you interpret and act in accordance with this Privacy Standard. You must also comply with all such Related Policies. Any breach of this Privacy Standard may result in disciplinary action.

3. SCOPE

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.
All managers are responsible for ensuring all Company personnel comply with this Privacy Standard and need to implement appropriate practices, processes, controls and training to ensure that compliance.
The Data Protection Manager (DPM) is responsible for overseeing this Privacy Standard and, as applicable, developing Related Policies (see Appendix).

Please contact the DPM with any questions about the operation of this Privacy Standard or the GDPR or if you have any concerns that this Privacy Standard is not being followed. In particular, you must always contact the DPM in the following circumstances:
***(a)** if you are unsure about what security or other measures you need to implement to protect Personal Data;*
***(b)** if there has been a Personal Data Breach;*
***(c)** if you are unsure on what basis to transfer Personal Data outside the EEA;*
***(d)** if you need any assistance dealing with any rights invoked by a Data Subject;*
***(e)** if you need help complying with applicable law when carrying out direct marketing activities; or*
***(f)** if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors).*

4.PERSONAL DATA PROTECTION PRINCIPLES
We adhere 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); and*
***(h)** made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).*
We are responsible for and must be able to demonstrate compliance with the data protection principles listed above. Under the GDPR, this is called Accountability.

5. LAWFULNESS, FAIRNESS AND TRANSPARENCY
Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

The "lawful basis" on which we most commonly Process Personal Data is:
(a) the Data Subject has given his or her Consent; or
(b) the Processing is necessary for the performance of a contract with the Data Subject; or
(c) the Processing is necessary to meet our legal compliance obligations (for example, keeping employee records).

"Transparency" means that, when we are acting as Data Controllers, we provide detailed, specific information to Data Subjects in the form of Privacy Notices. These Notices explain, in clear and plain language, how and why we will use, Process, disclose, protect and retain that Personal Data.

6. PURPOSE LIMITATION
Personal Data must be collected only for specified, explicit and legitimate purposes.
You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

7. DATA MINIMISATION
Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.
You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.
You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

8. ACCURACY
Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

9. STORAGE LIMITATION

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.
The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time.
You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

10. SECURITY INTEGRITY AND CONFIDENTIALITY

Personal Data must be secured against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.
We develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

You also have a responsibility for protecting the Personal Data we hold. You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested. You must exercise particular care in protecting Special Categories of Personal Data (also called Sensitive Data) from loss and unauthorised access, use or disclosure.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR.

11. REPORTING A PERSONAL DATA BREACH

The GDPR requires Controllers to notify any serious Personal Data Breach to the applicable national regulator and, in certain instances, the Data Subject. We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPM. You should preserve all evidence relating to the potential Personal Data Breach.

12. TRANSFER LIMITATION

The GDPR restricts data transfers to countries outside the EEA to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.
You may only transfer Personal Data outside the EEA with the consent of the DPM.

13. DATA SUBJECT'S RIGHTS AND REQUESTS

Data Subjects have 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 Company's Processing activities;*
***(c)** request details of the 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)** be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;*
***(g)** make a complaint to the supervisory authority;*
You 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).

You must immediately forward any Data Subject request you receive to the DPM.

14. ACCOUNTABILITY

The Company is obliged to implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Company is responsible for, and must be able to demonstrate, compliance with the data protection principles.
The Company's GDPR accountability processes include:
***(a)** appointing a DPM accountable for data privacy;*
***(b)** integrating data protection into internal documents including this Privacy Standard and Related Policies (see Appendix);*
***(c)** regularly training Company Personnel on the GDPR, this Privacy Standard and Related Policies and data protection matters including, for example, Data Subject's rights, Consent, retention policies and Personal Data Breaches; and*
***(d)** regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance.*

15. RECORD KEEPING

The GDPR requires us to keep full and accurate records of all our data Processing activities.

We keep records of our Processing, including records of Data Subjects' Consents (where appropriate) and procedures for obtaining Consents. These records include: 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's retention period and a description of the security measures in place.

16. TRAINING AND AUDIT

We are required to ensure all Company personnel have undergone adequate training to enable them to comply with data privacy laws. We also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.
You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

17. SHARING PERSONAL DATA

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

You may only share Personal Data 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 written contract that contains GDPR-approved third party clauses is in place with the third party.*

18. CHANGES TO THIS PRIVACY STANDARD

This Privacy Standard is reviewed at the management review at least one time a year. It does not override any applicable national data privacy laws and regulations in countries where the Company operates.

19. ACKNOWLEDGEMENT OF RECEIPT AND REVIEW

*I, [**EMPLOYEE NAME**], acknowledge that I received and read a copy of the Company's foregoing Privacy Standard, and understand that I am responsible for knowing and abiding by its terms. This Privacy Standard does not set terms or conditions of employment or form part of an employment contract.*

Signed …….

Printed Name …….

Date …….

APPENDIX

(list here any Company guidance notes on related aspects of IT. In addition to examples below, these could include current rules on: Social Media, Passwords, Encryption etc)

1. *Bring Your Own Device to Work (BYOD) Policy – internal use*
2. *IT Acceptable Use Policy – internal use*
3. *Data Retention Guidelines – internal use*
4. *Privacy Notice (or Privacy Policy) – for customers and clients*
5. *……*