EURA

Guide to the General Data Protection Regulation

6th Edition - 2026

Contents

Introduction

The GDPR is an EU Regulation (with a similar UK version) 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 (Section12) and an example of a company's Data Protection Policy (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. If you do require GDPR advice or are interested in obtaining EuRA's GDPR Compliance Certificate, please contact me at the email address below.

David Gourlay
EuRA Strategic Consultant - Legal Services

david.gourlay@mfmac.com

September 2026

1. The GDPR: a quick overview

In 2018, the GDPR introduced a single legal framework across the EU for handling personal data. The GDPR is also part of UK law and applies also in other EEA countries (Iceland, Norway and Liechtenstein). But the reach of the GDPR goes wider than these specific countries: businesses based elsewhere in the world, which offer services to EU residents, are also subject to GDPR rules.

Under the GDPR, there are **six principles** which govern the processing of personal data:

1. **Lawfulness, fairness and transparency** - you need a legal basis for processing an individual's data (e.g. consent or a contractual obligation) and you need to explain, in plain language, how you will use the data.

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 should 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 must have 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.

EU and UK GDPR Representatives

Organisations not established in the EU / EEA that are subject to the GDPR and which process personal data of EU / EEA residents generally must appoint a representative physically located in the EU / EEA if they offer goods or services to EU / EEA individuals or monitor their behaviour. The GDPR representative serves as a local contact for supervisory authorities and data subjects on matters relating to GDPR compliance.

In a similar way, organisations not established in the UK that process personal data of UK residents must appoint a UK based representative under the UK GDPR. This obligation is quite separate from the EU requirement to appoint a representative. The UK GDPR representative also serves as a contact point for the UK regulator, the Information Commissioner's Office, and data subject on matters relating to UK GDPR compliance.

Processing which is occasional, does not involve large-scale processing of special category or criminal offence data and is unlikely to result in a risk to individuals' rights and freedoms is exempt from the requirement to appoint a GDPR representative.

Your business should also be aware of the key concepts of **Privacy by Design** and **Privacy by Default** which are built into the GDPR. These require you to build privacy protections into systems and processes from the outset so as to ensure an adequate level of privacy for an individual's personal data, rather than adding them at a later date.

You must need to remember to carry out a **Data Protection Impact Assessment** or "**DPIA**" if your organisation intends to carry out any processing which is likely to result in a high risk to the rights and freedoms of individuals. For example, if you are thinking about processing involving the use of new technologies, or the novel application of existing technologies, including AI, you should undertake a DPIA before the data processing begins.

A template DPIA is available here: https://www.edpb.europa.eu/public-consultations/template-for-data-protection-impact-assessment_en.

Data Protection Authorities (DPAs) across the EU have stressed that the GDPR was not intended as a revolutionary change, but describe it instead as an "evolution" of data protection 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.

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. 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***. Nevertheless, both the controller and the processor can face potential penalties if things go wrong.

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

- A corporate client 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 contract between corporate client and RMC, and it is not uncommon to find that both corporate client and RMC are acting as ***controllers*** for different categories of data;
- A destination services provider (DSP) instructed by either a corporate 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 know 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.

If there are 250 or more employees in your business, your business is, in any event, required to document all its processing activities. For small and medium-sized organisations, if your business employs fewer than 250 people, you are only required to document processing activities that (1) are not occasional (e.g., are more than just a one-off occurrence or something you do rarely); or (2) are likely to result in a risk to the rights and freedoms of individuals (e.g., something that might be intrusive or adversely affect individuals); or (3) involve special category data or criminal conviction and offence data.

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)*
- What kind of personal data do you process? *e.g. only basic contact information or more detailed data?*
- 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*
- Does any data relate to criminal conviction or offence data?
- Do you hold any financial information? e.g. *customer credit card and bank account details or salary information, all requiring strong security measures*
- 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? e.g. do you store any data in the cloud such as with AWS or Microsoft Azure and do you know where that data is held?
- 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 EEA/UK?

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 be carefully checked to ensure that it complies with the definition above. If it does not, then the document wording should be updated or the business should rely on a different lawful basis.

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.

Because an individual must be able to withdraw consent at any time (and you must make the withdrawal process easy, clear, and immediate for them), you may find that consent is not the appropriate lawful basis to use for your processing

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. In practice, most relocation businesses prefer to rely on specific consents from individual assignees.

Before deciding to rely on legitimate interest, your business should carry out what is known as a "legitimate interests assessment" or "LIA". This requires your business to be satisfied that (1) a legitimate interest is being pursued by the controller or by a third party; (2) there is a need to process personal data for the purposes of that legitimate interest and (3) the interests, freedoms and rights of the persons whose information you want to use do not take precedence over the legitimate interest(s) of the controller or of a third party. The assessment should be documented by your business in line with the accountability principle.

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).

In addition to having a lawful basis for processing, where your business is processing any "special categories" data or criminal conviction and offence data, you need to exercise extra care and **also** identify a separate **condition** for processing under the GDPR. These do not have to be linked. For example, you can process special categories of data if you have the **explicit consent** of the individual concerned or processing is necessary to comply with **employment law**. The specific conditions for processing may vary from one Member State to another.

4. Your responsibilities to individuals

The GDPR gives individuals various rights 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, 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 and to receive a copy of their personal data, and other supplementary information.*

- **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)** - *individuals have the right to have their personal data erased although note that this does not apply while you are processing data as part of your contractual obligation*

- **purpose limitation** – holding a customer's consent to the processing of their data for one purpose (e.g. delivery of relocation services) does not entitle you to use their personal data for a separate purpose, such as adding their name to a marketing database. A separate purpose needs a separate consent.

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 regularly 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 (typically 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. Certain information must be contained in a Privacy Notice and businesses are obliged to use clear language and 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 <u>may</u> 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 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. A common retention period used by RMCs is seven years.

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, 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.

a) practical measures to protect personal data

Data protection authorities recommend that businesses should consider the following steps as part of compliance with the GDPR "Integrity and Confidentiality" principle:

- Back up your data – and make sure that the back-up works and is not connected to your live data source (protecting it from any malicious activity)
- Use strong passwords and multi-factor authentication
- Be wary of suspicious emails – train your staff to recognise phishing emails
- Install anti-virus and malware protection – and keep it up to date (and ensure that devices used away from the office are equally secure)
- Limit access to those employees who need it – different roles should have different access rights
- Do not keep data for longer than you need it – as well as complying with the GDPR "retention" principle, you will also have less personal information at risk if you suffer a cyber attack

b) handling a data breach

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 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 can be liable to pay damages or fines. The intention behind these 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 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 GDPR imposes strict rules on transfers of personal data to countries outside the EEA and UK.

"Consent" continues to be a valid basis for international transfers, but this is the 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 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. The European Commission has so far recognised the following countries: Andorra, Argentina, Brazil, Canada (commercial organisations only), Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, South Korea, Switzerland, United Kingdom and Uruguay, as providing adequate protection. 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 EEA 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.*** This is a complicated and time-consuming process and is not widely used.

- for **3rd party data transfers** - incorporate EU-approved ***Standard Contractual Clauses ("SCCs")*** in contracts with non-EEA/UK 3rd parties;

- for **data transfers to the United States** – the **EU-US Data Privacy Framework** provides a legal basis for transfers to registered businesses in the United States, otherwise European businesses have to fall back on SCCs for American data transfers.

One important legal change in the UK is the introduction of the **International Data Transfer Agreement**, which is used instead of EU SCCs for foreign data transfers from the UK. If a contract covers foreign transfers from both the EU and the UK, EU SCCs should be used along with a UK Addendum.

The GDPR 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 the legal requirement 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." You should also be clear about your conditions for processing any special categories of data and/or conviction or offence data. 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 receive information about how their personal data is processed. This is usually done in the form of an Employee Privacy Notice. Your business should also consider issuing policies on relevant aspects of employee rights and obligations, such as:

- any forms of employee monitoring which is carried out in your business;
- any company rules on 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. Your GDPR Documents and Records

Here is a summary of the GDPR documents and related records which most relocation businesses should have in place:

a) **Privacy Notice (*for your customers and contacts*)** – this will usually be publicly available via a link from your website;
b) **Privacy Notice (*for your own employees*)**;
c) **Data Protection Policy** – this will contain details of how your business protects personal data and complies with GDPR requirements and the obligations placed on all employees, such as Handling Data Breaches, Data Retention and Disposal and Data Subject Access Requests (though these are sometimes contained in separate policy documents);
d) **Supplier contracts** – every supplier with which your business shares personal data must have a contract with you containing the supplier's GDPR obligations;
e) **Record of GDPR Compliance** – a summary of your data processing (see "data audit" above), plus up to date records of staff training, data deletions and any data breaches or complaints;
f) **Business Continuity Plan**.

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 identical in all EU countries?

A main purpose of the GDPR was to strengthen and unify data protection law within the EU. However, the harmonisation of laws is not 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 continue, therefore, to be some national variations in data protection laws, but these variations have little practical impact on the steps being taken by relocation businesses to comply with the GDPR.

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

Not exactly. Following Brexit, the EU GDPR was incorporated into UK law as the **UK GDPR**, which sits alongside the UK's Data Protection Act 2018. For most UK organisations processing personal data in the UK, the relevant regime is therefore the **UK GDPR**, rather than the EU GDPR. The UK GDPR is very similar, but not identical, to the EU GDPR.

The EU GDPR can, however, still apply directly to UK organisations where its territorial scope is triggered, for example where a UK organisation offers goods or services to individuals in the EU or monitors the behaviour of individuals located in the EU.

The close alignment between the UK GDPR and EU GDPR enabled the UK to receive an EU **adequacy decision**, allowing personal data to continue flowing between the UK and the EU without the need for additional transfer safeguards.

3) Are large fines imposed for GDPR breaches?

There has been a lot of scaremongering on this issue, probably due to the maximum fines which DPAs can impose under the GDPR - up to **€20 million** or **4% of an undertaking's total worldwide annual turnover** (whichever is **higher**) for the most serious infringements. But, to date, the DPAs have focussed 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, in a recent 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 an organisation in the following circumstances:

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

You should also consider carefully where data is going to be stored in the "cloud". For example, if data will be held in the United States you will need to make sure that the international transfer of data is done in a way which is compliant with the GDPR. Your privacy notices should also make individuals aware of any such transfers.

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 we are seeing 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".

7) What other action might we face if we breach the GDPR?

Whilst DPAs typically prefer dialogue to enforcement action where appropriate, you should bear in mind that DPAs do have the power to investigate organisations, conduct audits, issue warnings and reprimands, require the deletion or restriction of personal data, suspend date processing or data transfers and order corrective actions as well as impose fines.

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 the following countries:

- 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/
- Iceland: https://island.is/s/personuvernd
- Ireland: http://www.dataprotection.ie/
- Italy: http://www.garanteprivacy.it/
- Latvia: http://www.dvi.gov.lv/
- Lichtenstein: https://www.datenschutzstelle.li/
- Lithuania: http://www.ada.lt/
- Luxembourg: http://www.cnpd.lu/
- Malta: http://www.dataprotection.gov.mt/
- Netherlands: https://autoriteitpersoonsgegevens.nl/nl
- Norway: https://www.datatilsynet.no
- 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 Protection Impact Assessment (DPIA) - an assessment which is designed to help an organisation understand how a project, system, or process could affect people's privacy and what measures are needed to eliminate or reduce any risks that are identified.

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

EU-US Data Privacy Framework - 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 certified companies in 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 Data Protection Policy

[insert COMPANY NAME] - Data Protection Policy

(an outline for employees of how the Company complies with the GDPR)

1. EXPLANATION OF LEGAL TERMS USED IN THIS DATA PROTECTION POLICY

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.*
Criminal Convictions Data*: Personal Data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings.*
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 a relocation management company. The Processor must comply with the GDPR, but its legal obligations are secondary to those of the Controller.*
Data Privacy Impact Assessment (DPIA): *tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.*
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. A similar GDPR exists under UK law.*
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 by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.
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.*
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 Data Protection Policy 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 Data Protection Policy sets out how we handle the Personal Data of our customers, prospective customers, suppliers, employees, workers, business contacts *and other third parties. It applies to all Personal Data we Process regardless of the media on which that data is stored.*
This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users, or any other Data Subject.
This Data Protection Policy applies to all Company personnel. You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you to ensure that the Company complies with the GDPR and other applicable laws. Your compliance with this Data Protection Policy is mandatory. Related Policies, referred to in the attached Appendix, are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all such Related Policies. Any breach of this Data Protection Policy may result in disciplinary action.

3. SCOPE

We recognise that the correct and lawful treatment of Personal Data will maintain trust and 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 Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.
The Data Protection Manager (DPM) is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies (see Appendix).
Please contact the DPM with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this Data Protection Policy is not being followed. In particular, you must always contact the DPM in the following circumstances:
(a) if you are unsure of the lawful basis on which you are relying to process Personal Data (including the legitimate interests used by the Company)
(b) *if you are unsure about what security or other measures you need to implement to protect Personal Data;*
(c) *if there has been a Personal Data Breach;*
(d) *if you are unsure on what basis to transfer Personal Data outside the EEA/UK;*
(e) *if you need any assistance dealing with any rights invoked by a Data Subject;*
(f) *if you need help complying with applicable law when carrying out direct marketing activities; or*
(g) *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.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK 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 "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); or
(d) to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects..

You must identify and document the legal ground being relied on for each Processing activity.

When considering relying on consent, you must understand that a Data Subject consents to Processing of their Personal Data if they clearly indicate agreement to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity will not be sufficient to indicate consent. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. 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.

When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies and privacy guidelines, so that the Company can demonstrate compliance with Consent requirements.

"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.

If you are collecting Personal Data from a Data Subject, directly or indirectly, then you must provide the Data Subject with a Privacy Notice in accordance with our Related Policies and privacy guidelines.

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.

If you want to use Personal Data for a new or different purpose from that for which it was obtained, you must first contact the DPM for advice on how to do this in compliance with both the law and this Data Protection Policy.

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.
You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.
You will ensure Data Subjects are provided with information about the period for which data is stored and how that period is determined in any applicable Privacy Notice.

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) and Criminal Convictions Data from loss and unauthorised access, use or disclosure 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/UK 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/UK 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)** implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;*
***(c)** integrating data protection into internal documents including this Data Protection Policy and Related Policies (see Appendix);*
***(d)** regularly training Company Personnel on the GDPR, this Data Protection Policy and Related Policies and data protection matters including, for example, Data Subject's rights, Consent, retention policies and Personal Data Breaches; and*
***(e)** 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.

You must 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. USE OF ARTIFICIAL INTELLIGENCE (AI)

We comply with all relevant legislation related to the use of AI and, specifically, we:
a) *analyse the internal and external use of AI tools and/or systems and assess risks;*
b) *ensure that clients and customers are aware when they are interacting with our AI system and not with an individual;*
c) *define, implement, and communicate AI principles and guidelines; and*
d) *train all employees on AI principles and guidelines to create risk awareness (verifiable and documented).*

17. 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 Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

18. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

We are required 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.

You must assess what Privacy by Design measures can be implemented on all programmes, systems or 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.*
(d) *The risks of varying likelihood and severity for rights and freedoms of the Data Subject posed by the Processing.*

The Controller must also conduct a DPIA in respect to high-risk Processing.

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data

19. DIRECT MARKETING

We are subject to certain rules and privacy laws when engaging in direct marketing to our customers and prospective customers (for example when sending marketing emails or making telephone sales calls).

For example, in a business to consumer context, a Data Subject's prior consent is generally required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt-in" allows an organisation to send marketing texts or emails without consent if it:
(a) *Has obtained contact details in the course of a sale to that person.*
(b) *Is marketing similar products or services.*
(c) *Gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent marketing message.*

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 always be promptly honoured. If a customer opts out of marketing 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.

You must comply with the Company's guidelines on direct marketing to customers and you should consult your line manager if you are unsure regarding how to comply with either the Company's guidelines or the law.

20. 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 the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

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.*

21. CHANGES TO THIS DATA PROTECTION POLICY
This Data Protection Policy 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.

22. ACKNOWLEDGEMENT OF RECEIPT AND REVIEW

*I, [**EMPLOYEE NAME**], acknowledge that I received and read a copy of the Company's Data Protection Policy dated [INSERT DATE], and understand that I am responsible for knowing and abiding by its terms.* I understand that this Data Protection Policy *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 – for customers and clients*
5. *……. etc.*