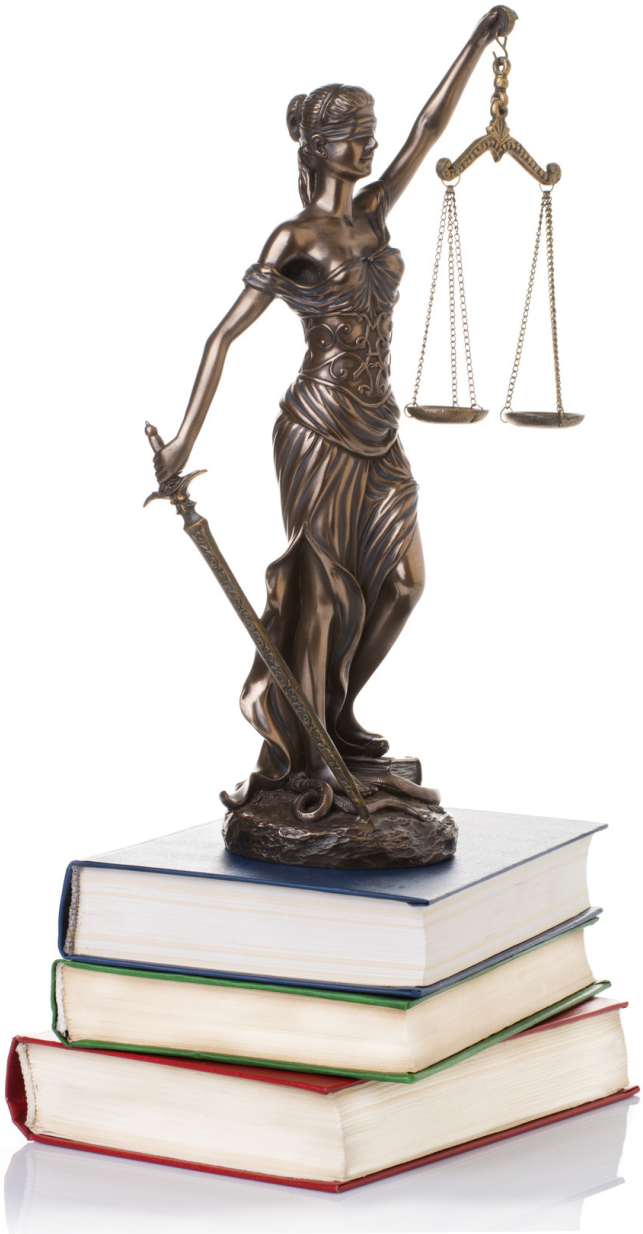
Guide to Legal Compliance



5th Edition 2024

The EuRA Guide to Legal Compliance

Contents

Introduction

Welcome to the 5th edition of our Guide to Legal Compliance!

The good news is that since the publication of our 4th edition in 2022, the legal landscape for relocation businesses has remained relatively unchanged. This is in marked contrast to previous years, when we were bombarded with new legislation and guidelines, particularly in the field of data protection. Our industry has been largely successful in adjusting to the requirements of the GDPR followed by the challenges of Brexit.

As always, the purpose of the Guide is to provide EuRA members with an introduction to the main legal issues which affect relocation businesses. It is impossible, of course, for any guide to cover all relevant law, particularly as much of this is particular to individual countries. Instead, our objective is to offer a practical introduction to the legal issues which can arise irrespective of where in Europe (or further afield) you deliver services.

It is quite common for companies based outside Europe to wrongly assume that there is something called "European law", but this is far from the case. In many areas of business activity, the law is not even EU-based but is governed by national laws, and international businesses require to obtain local legal advice. Where EU legislation does apply, it comes in two forms: "**Regulations**" are directly enforceable in all EU countries whereas "**Directives**" set out a policy goal, but it is left up to individual countries to enact legislation.

Following Brexit, EU law no longer applies in the United Kingdom. However, in many legal areas, such as the GDPR, EU law has now been incorporated directly into UK law, and it's likely that we will continue to see some harmonisation of EU and UK laws for some years ahead.

The legal topics covered in this Guide are:

1. Contracts with your clients
2. Protecting personal data
3. Anti-bribery & corruption
4. Relocation & tax
5. Insurance
6. Cross border employment and start up issues
7. Expat tenancies
8. Other legal issues;
    (a) Anti-money laundering
    (b) Competition law
9. Legal compliance and the EuRA Global Quality Seal

In a Guide of this nature, it is impossible to avoid the use of some legal terms. To assist you, a Glossary of Terms is included at the end of the Guide.

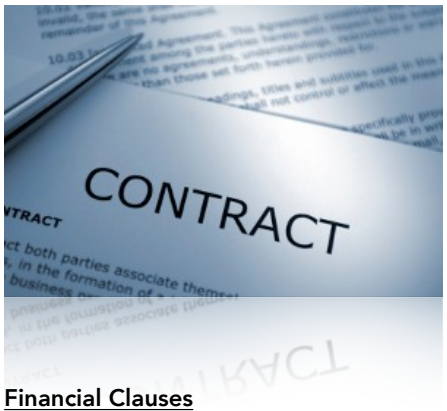
We hope that this Guide will be a useful starting point for you in addressing the legal issues which are most likely to affect your business. This Guide is supplemented by a compliance advice service for EuRA members. We cannot provide specific legal advice, but we believe that there is value in highlighting and discussing the legal issues which are most likely to affect our members. We hope that you agree, and we will always welcome your feedback on how this Guide can be improved and developed in the future.

Gordon Kerr
Strategic Consultant - Legal Services

1. Contracts with your clients

a) Corporate Clients

On one view, contracts only matter when things go wrong: for example, when an invoice is not paid or when there is a dispute over a service "failure". But a well-prepared contract should actually make life easier for both parties, as it will clarify upfront exactly what services will be delivered for what fees and will create a mechanism for resolving any disagreements as amicably as possible.



The most common practical problem today, particularly for DSPs, is that lengthy, highly technical, "standard agreements" are produced by the legal departments of RMCs or corporate clients and there may be very limited opportunity to negotiate terms. Even if such an opportunity exists, it is just not commercially viable to have every draft agreement fully vetted, on your behalf, by a lawyer.

So, if you are checking over a contract without the benefit of legal advice, what are the most important things you should be looking for?

Financial Clauses

These clauses will probably be the starting point for your review of a new agreement, and you will want to be clear about several things:

- What are the payment terms - e.g. 30, 45 or 60 days from the client's receipt of your invoice?
- Are you entitled to interest on any late payments?
- Are you satisfied that you can comply with the details of the client's invoicing process? - e.g. a complicated process may mean payment delays which are outside your control;
- Will any third-party costs require to be advanced by you and how quickly will you be reimbursed for these? Will you be paid interest on these advances?
- Are you entitled to pro-rata payment for any work which is cancelled by the client prior to completion of service by you?
- Is the client entitled to refuse payment for any "late" invoices submitted by you, e.g. more than 90 days after service delivery?
- Are there any penalty (or bonus) terms - e.g. a fee reduction (or addition) based on service quality scores? Are you comfortable that these are clear and will work fairly in practice?
- Is the client entitled to a discount based on volume of cases? If so, it is preferable that the discount should apply only to cases received after the agreed threshold has been reached, rather than applying to all cases.
- Are you protected against exchange rate fluctuations?

Key Performance Indicators (KPIs), contained in an Agreement, can assist both parties to focus on the things that really matter in terms of achieving a successful business relationship. But problems arise when the wording of KPIs becomes so detailed and complicated that they almost become meaningless. Particular care has to be taken when failure to achieve KPIs can incur financial penalties. If there is to be a link between KPIs and fees, you may want to also have the opportunity to earn bonuses for high performance and not simply be subject to potential penalties.

Of course, it is not only the financial clauses in Relocation Service Agreements which can cause you difficulties. Below are some of the other main clauses which require particular attention:

Length and renewal

Is the agreement for an indefinite period, subject to notice of termination (e.g. 60 days) by either party – or is this a fixed term agreement (e.g. 3 years) with options to extend? Are your prices fixed for the period of the contract or is there a mechanism for adjusting these (e.g. every 2 years)?

Choice of law and courts

The agreement should set out which law will apply to the contract (e.g. English, French, German etc) and which country's courts will have jurisdiction to deal with disputes. Ideally, you will want the convenience of being able to use your national law and local courts. However, an international client will generally seek to link their relocation services contracts to the country or state of their global headquarters and it can sometimes be difficult to negotiate any change to this.

Employee background checks
It is increasingly common to find that global relocation service contracts impose obligations on "the supplier" to carry out a variety of checks on its employees and contractors. These obligations can be particularly stringent when the client is a US-headquartered corporation. But, employee background checks and drug tests, which may be commonplace in the US, can often be impossible to replicate in countries where privacy laws are stronger. In EU countries, for example, individual privacy rights are strongly protected and you should not accept obligations in a contract which are contrary to your national privacy laws.

Data Protection Clauses

DP clauses in contracts are getting longer and more complicated. This is because the general obligations placed upon suppliers, to handle personal data correctly, are now enhanced by very specific obligations arising, for example, from the EU General Data Protection Regulation ("GDPR") and EU Standard Contractual Clauses.

Wading through several pages of DP clauses is an unattractive prospect, but for EU-based businesses, already familiar with the high levels of data protection imposed under EU law, there should not be any real surprises contained in the contract wording. However, it always pays to read these clauses carefully, looking out for anything which you are uncomfortable with, for example:

- The client may impose audit and penetration testing requirements, which may be unreasonable in terms of potential disruption and cost to your business;
- Potential penalties and indemnities for breaches of DP obligations may be unreasonable.

A client would reasonably expect you to accept the following basic obligations:

- To use personal data of assignees only as necessary for the purposes of providing authorised services and for no other purpose;
- To maintain safeguards to protect personal data against loss, disclosure or access by third parties;
- To comply within a reasonable timeframe with any request from client or the assignee for access to or deletion of their personal data;
- To retain personal data only for as long as is necessary for the provision of relocation services or as required by law;
- Except with consent of client, not to a) disclose personal data to any third party and b) transfer personal data across international boundaries;
- Upon reasonable notice, to permit auditing by client of your data processing facilities and relevant data files.

Further information on insurance for relocation businesses is contained below .

Anti-bribery clauses

Under the UK Bribery Act, which is the nearest thing we have to a global standard for anti-corruption law, clients may be held liable for failure to prevent bribery by their contractors. This means that relocation service agreements will usually contain very specific compliance obligations on suppliers. It is important to be aware of any penalties or indemnities which the client can impose for non-compliance. Could these be damaging to your business?

Further information on Anti-Bribery law is contained below.

Insurance clauses

Relocation service contracts will normally specify the types of insurance cover which the supplier must have in place and set financial levels for each category of cover (e.g. professional indemnity cover of not less than €1 million per claim). The wording of insurance clauses can be very technical, and you may wish to refer the contract wording to your insurance broker, who can confirm if you are currently compliant or whether additional cover will be required - and at what cost.

Your insurance cover should tie in with any “limitations on liability” contained in the agreement, e.g. financial caps on liability. Does your business have sufficient insurance coverage to ensure that it has the financial capacity to satisfy its liabilities under the contract?
Further information on insurance for relocation businesses is contained below [insert link here].

Penalty Clause

These are clauses which impose a financial penalty on the supplier for a failure to comply with particular obligations under the contract. It is clearly important to be aware of any penalties contained in a contract. In many countries, a contractual penalty is unenforceable unless it represents a genuine estimate of the likely cost to the client of the breach of contract; i.e. it should not be "penal" in nature.

Indemnity Clause

If you breach the Agreement with your client, and this contains an indemnity clause, you may have liability for all costs incurred by the client, even where these costs may have been unforeseeable or excessive in your view. In this way, an indemnity clause can result in higher costs for your business than would arise if a court were assessing reasonable damages in the traditional way. For example, you may have liability for your client’s total legal costs, even where these appear to be excessively high.

Ideally, you will wish to delete any indemnity clause. In reality, if you cannot achieve this, you should at least be aware that the cost of any contractual non-compliance may be higher than you would normally expect.

Force Majeure Clause

Force majeure is a legal concept that allows a business contract to be suspended or terminated when the contract is seriously affected by a major external event which is outside the control of either party. For example, if you have relocation contracts in place that are affected by coronavirus — through employee illness, quarantine, or governmental restrictions on trade or travel — then force majeure may give you some legal protection against a claim that you have failed to deliver agreed services.

Intellectual property

Are there any intellectual property rights issues? If yes, how will these be dealt with?

Disputes and arbitration

A clause which sets out a simple process for parties to attempt to resolve disputes amicably can be valuable. The next step, short of court action, will often be an arbitration process. Arbitration can also be very useful, but less so (from a European perspective) if the arbitration location is stated to be the client's HQ location, e.g. in the United States.

Negotiating the removal of "unreasonable" contract terms

The starting point, of course, is that you want to do business with this new client. But a contract which you believe contains unreasonable terms will require you to have a follow-up discussion with the client. You should highlight the clauses which are causing you serious concern and explain why.

It is not uncommon to find that inappropriate clauses have been copied from a previous contract in error and there should be no difficulty in having these removed or amended. On the other hand, it is clearly more challenging to negotiate contract wording which the client imposes in all their contracts as a "standard term". In this latter situation, you may still be able to have a clause removed where it is inconsistent with your national law (e.g. an obligation to carry out certain "employee background checks").

Another approach, which may help to break a deadlock, is to accept a "side letter" from the client, confirming that a particular clause will not be enforced in practice (e.g. a client's standard clause relating to annual penetration testing of your IT systems). This can be a useful compromise in situations where the client is otherwise refusing to amend the wording of its standard clauses.

Avoiding contract pitfalls

Here are two common pitfalls that frequently arise during the contract negotiation stage, and some suggestions to address them.

Scenario 1: Incorporating tender documents into the contract

"We have no time to draft the specification and delivery schedules in our contract. Can we just use the responses submitted during the tender stage by including it in those schedules?"

While convenient, this is a risky approach because tender documents:

- Can lack certainty and detail. Ambiguous drafting in a contract is likely to cause disagreement in future. A contract may be unenforceable if its terms are too uncertain.
- May have broad sweeping statements. For example, "we want to be your trusted supplier to help deliver all your business' needs relating to [relocation project] and will do all we can to help you achieve that objective". There is a lack of clarity about the precise obligations (and deliverables).

Suggested approach:

- Avoid copying and pasting wording from tender documents into the final contract. If you do use wording from these documents, make the drafting as clear and certain as possible.
- Get input from relevant stakeholders in the business when drafting these schedules. Check that those involved in the actual delivery of the services are satisfied that the drafting accurately represents what they need to do and that they do not create an unreasonably onerous obligation.

Scenario 2: Statements made during the negotiation process, but not written into the contract

"The supplier gave some oral assurances during a meeting about minimum volumes. Would this be a term of the contract? Can we rely on it?"

In most cases, no, you would not be able to rely on it because:

- Most contracts will have what is known as an "entire agreement" clause which generally provides that all the agreed terms of the contract are to be found in the contract, and nowhere else.
- The effect of this is that, if something is not written in the contract, it is not a term of the contract. So the parties cannot rely on it.

Suggested approach: if you want an undertaking to form part of the contract, make sure this is written into the agreement.

b) Personal Clients

While our main focus in this Guide is on contracts with companies (either RMCs or corporate customers), it is worth looking at the key issues you will wish to cover when contracting direct with an individual. For example, while you may be reasonably relaxed about obtaining payment from a well-established company, you will probably want to obtain a substantial upfront payment from an individual client.

Typically, you would issue Terms and Conditions ("T&Cs") to a prospective new client, covering some or all of the following points;

- Your service will not start until your client has returned a signed copy of the T&Cs and paid a registration fee;
- A clear statement of the service to be provided, the registration fee and the final fee
- Your full fee will be payable whether or not the property chosen by the client is introduced or negotiated by you;
- Payment terms and VAT;
- Governing law and jurisdiction of your local courts;
- Other clauses may deal with a range of other issues which are relevant to your relationship with the client, such as: data protection, money laundering checks, exclusions of liability etc.

As a general rule, it is wise to use plain language in T&Cs and to avoid wording which is complicated and difficult for an average person to understand. As a personal consumer (unlike a business customer), your client may be able to claim that they did not fully understand the meaning of a clause in your T&Cs and challenge the enforceability of an "unfair" contract term under consumer protection law.

2. Protecting Personal Data

Overview

In order to deliver an effective relocation service, your business probably collects and uses a great deal of personal information relating to your customers and their families. You will hold full contact information. You may also hold their dates of birth, their children's names and sometimes, their medical history. Data protection law refers to this type of information as "personal data" and imposes stringent legal obligations on all businesses which handle such data.

Compliance with data protection law has been pushed up the agenda of most businesses, across all industry sectors, since the introduction, in May 2018, of the EU's General Data Protection Regulation (GDPR). Following Brexit, there is now a similar UK GDPR.

The legal overview below is split into the following sections:

a. The GDPR

b. Practical steps to protect personal data

c. Data protection and your contractual obligations

d. Privacy rights of your own employees

e. Other data protection laws which may affect your business

f. List of Data Protection Authorities in Europe

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 is where things get just a bit 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.

We also need to be clear about what exactly is meant by "processing" and what is included in the term "personal data":

- **"processing"** is any interaction with personal data, including collecting, storing, using, altering and deleting;
- **"personal data"** is information relating to a living individual who can be identified from the data, including e.g. contact details, photographs, correspondence and biometric data; and
- **"special category** (i.e. sensitive) **personal data"** includes information on racial/ethnic origin, religion, sexual life and health issues, so needs to be treated with greater care than other personal data.

Businesses which process personal data in Europe need to be registered with a national data protection authority. Further information on registration and other legal requirements is contained on the national websites listed at section f) below.

a) The GDPR

The GDPR replaced existing national data protection laws across all EU member states and raised the bar for data protection and privacy. The overriding purpose of the law is to ensure that companies take reasonable measures to keep personal data secure, whether that data is contained in electronic format or in an old-fashioned paper file. Section b) below ("Practical steps to protect personal data") describes some of the ways that you can protect data.

Understanding the GDPR "Principles"

It is easy to become overwhelmed by the 261 pages of the GDPR. But everything flows from six underlying "Principles" governing 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 can only collect and process personal data for "specified, explicit and legitimate" purposes.

3. **Data minimisation** - you can only collect data which is "relevant" and is "limited to what is necessary".

4. **Accuracy** - all data held by you should be 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 latter requirement is called "accountability" and is a key element of the GDPR.

Is Your Business GDPR-Compliant?

In assessing your level of GDPR compliance, below are some key questions for your business to consider whenever you are acting as a data controller (and these obligations may also apply to data processors under the terms of your client service contracts):

1. Are you clear about:

a) what types of personal data (including sensitive personal data) are held and processed by your Company?
Unless you have clarity about the data flowing in and out of your business, you cannot be sure that you are GDPR-compliant – so this is your starting point.

b) the various ways in which personal data is obtained by your business?
e.g. obtained in writing, by telephone, via a website, via social media, via CCTV or other recording devices, etc

c) how the data is "processed" by your business?
Data is processed if it is obtained, recorded or held or if any "operation" is carried out on the data, including organising, altering, using, disclosing or destroying the information.

d) why the data is processed?
i.e. the specific purposes for which your organisation requires the personal data.

e) how and where personal data is held by your business?
e.g. electronically or as hard copies or both? on your premises or remotely?

2. Are your data privacy notices up to date and do you know how and where these are used (*e.g. on your website, in customer or supplier contracts, in employment contracts)*?

3. Do you use consent forms *(e.g. to seek a customer's consent for processing their personal data)* and what form do these take *(e.g. stand-alone consent forms or part of your business terms and conditions, contracts, privacy policies or data protection policies)*?
If you use tick boxes in consent forms, you should ensure that these require the customer to "opt-in" and you should not rely on simply providing an "opt-out" option. You should also ensure that there is information on how the customer can withdraw consent in future.

4. Do you provide DP guidance notes and staff training in relation to:
- keeping personal data up to date?
- removal or correction of data?

- security procedures (including specific guidance on "sensitive personal data")?
- dealing with subject access requests *(e.g. when a customer asks for details of their personal information held by you)*?

5. Do you have data retention policies and procedures, including:
    - how long your business retains personal data?
    - why you retain personal data for any stated period (e.g. obligation to retain certain records for statutory compliance reasons)?
    - how you ensure that personal data is deleted at the end of your retention period?

6. Do you keep records of;
    - any subject access requests in the past 12 months
    - any non-compliance or allegation of non-compliance with your data protection obligations?
    - any personal data audits undertaken by your organisation?

7. Do you have a disaster recovery plan for your business?
(including procedures for ensuring the internal and external security of hardware, software and data, including procedures for preventing unauthorised access, preventing the introduction of a virus and the taking and storing of on-site and off-site back-up copies of software and data).

8. If you share personal data with third parties (e.g. contractors, suppliers)
    - what personal data do such third parties have access to?
    - is there a specific service need for these third parties to access the data?
    - do your contracts with these third parties contain appropriate data protection obligations?

9. If you ever transfer personal data outside the EEA/UK (the European Economic Area is EU countries, plus Iceland, Liechtenstein and Norway), are you clear about your additional legal obligations to safeguard the data?
(e.g. *you may need to use EU Standard Contractual Clauses or UK International Data Transfer Agreement.)*

10. Do your contracts (e.g. with employees, customers and suppliers) contain up-to-date data protection and privacy clauses?

12. Are you aware of your responsibility to ensure that, as new processes, software etc. are rolled out, key data protection principles, such as inserting a reasonable timetable for deletion of personal data, now require to be built in to the new processes? *(this is called "Privacy by Design").*

GDPR: frequent Q&As

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

1) following Brexit, does the GDPR apply to the UK?
The UK's Data Protection Act 2018 allows for the continued application of GDPR standards and the GDPR is incorporated into the UK's domestic law. So, the UK and EU data protection regimes should continue to be aligned for the foreseeable future and there are no restrictions on the free flow of personal data between the EU and the UK.

2) does the GDPR apply to "cloud computing"?
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.

3) do we need to appoint a Data Protection Officer (DPO)?
Under the GDPR rules, it is unlikely that any relocation business would require to appoint a DPO, though some may decide to go down this route voluntarily.

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. You should not use the term "Data Protection Officer" for this role, as this has a defined meaning and specific legal responsibilities in the GDPR. Instead, many firms use the term "Data Protection Manager".

4) does the GDPR allow "data aggregation"?
If you enter a contract with an online systems provider which contains a "data aggregation" clause, this allows the website owner to create and use, for its own purposes, statistical data based on the content placed on its system by your business. This collection of "aggregated data" does not breach the GDPR *provided that* the website owner complies with what the GDPR calls "pseudonymisation". This means that the data cannot be linked to individuals.

The wider commercial aspects which EuRA members may want to consider here, include:

1. It is now quite common to find an aggregate data clause in cloud, software and other technology agreements, giving the vendor/provider the right to compile, collect and use aggregate data for their own business purposes;

2. Some customers push back on the clause as a matter of policy, citing underlying concerns about confidentiality and also a reluctance to see a third-party benefit from their data;

3. On the other hand, vendors will argue that, as their specific customers are not identified, there is no potential harm to the customer and that pricing would have to be increased if the vendor was unable to exploit the data for commercial purposes.

5) 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 now see more 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".

b) Practical steps to protect personal data

The GDPR requires your business to take "appropriate technical and organisational measures" to secure personal data. This is a very general and non-specific requirement, which leaves individual businesses with the task of deciding what security levels are appropriate. For example, a higher standard of protection will be required if you hold records on medical conditions or collect bank account information compared with a business which holds only basic contact information on its customers.

To determine whether your business has adequate data security in place, we recommend that you address the following questions:

- ***What systems and processes are currently in place to protect personal data?***

Personal data must be kept secure at all times. For example:

- Computers and files should be password protected.
- Personal data on laptops and other portable devices should be kept to a minimum.
- Manual filing cabinets containing personal data should be locked and only accessible to authorised personnel.
- Confidential documents should not be left unattended on desks.
- Personal data should be removed promptly from printers and photocopiers.
- Your staff should be trained to handle personal data safely and securely.

When a business sends personal data, it must be done in a secure way. Personal data must be disposed of securely (for example, by shredding, placing in confidential waste bags, destroying or securely deleting electronic files). Confidential papers should not be put in the recycling bin.

Security breaches (such as accidentally losing personal data) should be reported immediately to senior management and there may be a requirement for your business also to report the breach to your client, to your national data protection authority and/or to affected individuals.

- ***Are You Allowed to Collect This Data?***

A business can only collect personal data if it has a legitimate reason for doing so (for example, because an individual/family is to be provided with assistance to find suitable housing).

When you collect data about an individual, the data controller needs to tell that individual what you intend to do with their data (for example, as part of the information required in order to deliver a relocation service). If you later want to use the data for different purposes (for example, to deliver a completely unrelated service), the individual must be informed once again.

You should only collect information that you require at that particular time. For example, a customer's bank details should only be requested when it is certain that these will be required in order to deliver a particular service - and not as part of a general information-gathering exercise.

If you want to use someone's data for marketing purposes, the individual must be informed - and provide explicit consent.

- ***Are you <u>using</u> data lawfully?***

You are allowed to use someone's personal data if they have given their consent, but data should only be used for the specific reason that it was collected. For example, personal information provided for service purposes cannot be retained for marketing purposes without the specific consent of the customer.

If you want a third party to manage data (such as carrying out payroll services), you still remain responsible for protecting the data and will need to enter into a written contract with the third party.

Additional restrictions (and consent requirements) apply to data transfers across international borders. For example, if you are asked to transfer personal data from an EU country to the United States, you should be checking that your contract with the US-based business includes the EU's Standard Contractual Clauses.

- ***Are you <u>storing</u> personal data lawfully?***

All data held by you should be accurate and up to date. Databases should be regularly cleaned and out-of-date information must be deleted. Data should only be held for as long as it is required and for the reason it was collected. It should not be held on the basis that it may be needed for another reason at some time in the future.

- ***Are you protecting data when working away from the office?***

In practice, many serious security breaches have arisen from something as simple as an employee leaving a laptop or briefcase in a café or on a train.

When working away from the office or in public areas, you should:

- Ensure personal data stored on portable devices such as laptops, smartphones, tablets or memory sticks is encrypted and kept secure at all times.
- Avoid leaving papers or electronic devices lying around.
- Make sure members of the public cannot see confidential documents or computer screens; and
- Avoid talking about confidential matters when members of the public may be able to hear.

- ***Are you responsive to personal data enquiries?***

You should have a system in place to respond to individuals who request details of the personal information that you hold on them. The request should normally be passed to the person within your business who has responsibility for data protection issues. If your business is only the "data processor", the request should be passed immediately to the "data controller".

- ***Are you aware of the penalties for data protection failures?***

There can be serious financial, commercial and reputational implications for your business (including possible criminal penalties and fines) if personal data is not handled properly. Under the GDPR, fines for data protection breaches have risen substantially.

c) Data Protection and Your Contractual Obligations

All relocation service contracts entered by DSPs, either with employers or with RMCs, should now contain mandatory data protection clauses. A similar obligation is placed on DSPs to have GDPR-compliant clauses in place when entering contracts with contractors, such as independent home search consultants.

The intention behind the GDPR's stricter rules is that controllers (e.g. a corporate employer or an RMC) and processors (e.g. a DSP) will have a clearer understanding of their respective obligations and responsibilities.

Contracts must set out the content and duration of the data 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 the national data protection authority;
- 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.

d) 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.

- **GDPR Requirements**

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.

- **Employee Checks**

Another aspect of employee privacy which can cause challenges for European relocation businesses is the issue of employee checks. It is common to find that relocation service contracts impose obligations on the supplier to carry out a variety of checks on its employees and contractors. These obligations can be particularly stringent when the client is a US-headquartered corporation. But, employee background checks and drug tests, which may be commonplace in the US, can be impossible to replicate in European countries, where privacy laws are stronger.

For example, UK employers and service providers requiring individuals to obtain and disclose certain protected data, such as criminal records checks or barring records, are committing a criminal offence. Only employers in certain sensitive occupations can lawfully obtain enhanced criminal record checks.

Privacy rights are now strongly protected and relocation businesses should ensure that their policies on employee background checks and the relevant clauses in their relocation service contracts are consistent with current law.

e) Other Data Protection Laws Which May Affect Your Business

In addition to the GDPR, you should become familiar with the following laws and protocols relating to data protection:

- The EU and UK maintain approved lists of countries which provide "adequate protection" of personal data. Personal data can be transferred to suppliers in these countries without the need for the extra protections mentioned below. To date, a relatively small number of countries have received approval. These include: Argentina, Canada, Israel, Japan, New Zealand, South Korea, Switzerland and Uruguay.

- But, for example, at the present time, Australian privacy law is not considered to provide an adequate level of protection for personal data from the EU. This means that personal data transfers from EU countries to non-approved countries (such as Australia, China and India) must be protected by one of the specific methods approved by the EU Commission. These are:

    - For internal data transfers (within a group of companies) - implement corporate rules for transferring data, in the form of EU-approved *Binding Corporate Rules*;

    - For 3rd party data transfers - incorporate EU-approved *Standard Contract Clauses (SCCs)* in all contracts with 3rd parties which make reference to the transfer of personal data.

- Data transfers to the United States are allowed, without the need for SCCs, provided that the US company receiving the data is registered under the EU-US Transatlantic Data Privacy Framework (and its UK-US equivalent).

- Data Transfers from the UK to non-approved countries should use the UK International Data Transfer Agreement, which is the UK equivalent of EU SCCs.

- DP laws in non-EU Countries - because the EU sets very stringent standards of data protection, it is highly likely that compliance with EU legal standards will be sufficient to ensure that your business is compliant with relevant national laws when you are operating outside the EU. However, unexpected challenges can sometimes arise and this can be illustrated by a Russian data privacy law which required that a Russian citizen's personal data which is being transferred to a foreign server must also be held on a server in Russia. When operating in a new country, it is important to have a reliable source of local advice on this type of issue.

f) Data Protection Authorities in Europe

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

- 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

3. Anti-Bribery and Corruption

Knowledge of bribery law - and compliance with it - is important for relocation businesses of all sizes. For RMCs, there is potential liability for the corrupt actions of an individual contractor somewhere in the global supply chain. And for DSPs, there is the need for greater checking on work which is sub-contracted and also for ensuring that, within your business, all employees are clear about what activities are now unacceptable under current bribery laws.

It is no longer sufficient to simply declare that "I have never received or paid a bribe". Today, international law requires you to go a step further and have systems in place for preventing bribery, which could be taking place without your direct knowledge. This stronger legal regime can render you liable not only for the actions of your employees, but also for any corrupt actions on the part of your contractors.

National enforcement agencies, such as the UK's Serious Fraud Office (SFO), are now very serious about prosecuting bribery offences. For example, following an SFO investigation, Rolls-Royce was fined almost £500 million in 2017 for conspiracy to corrupt and failure to prevent bribery in seven countries (China, India, Indonesia, Malaysia, Nigeria, Russia and Thailand). Relocation firms, often under pressure to deliver fast solutions in challenging locations, must be vigilant about ensuring the adequacy of their anti-bribery and corruption procedures.

The defence for an organisation which finds itself under investigation is to prove that it had in place "adequate procedures" designed to prevent persons associated with it from carrying out bribery activity. Based on your assessment of risk, it may be advisable to carry out an annual review and a regular update of the adequacy of your organisation's anti-bribery procedures.

It is now well established that a company's anti-bribery policy, which simply gathers dust on an office shelf, offers no legal protection to your business if an employee or your contractor engages in corruption. The policy must be shared, explained, discussed and reviewed. It must become part of corporate culture, from top to bottom, and be shared with external contractors and agents.

One practical problem is that corporate anti-bribery policies are growing in length. Legally, if nobody is actually reading your long and detailed anti-corruption policy then the policy offers little defence against prosecution. A good recommendation is to stick with a short policy, accompanied by some simple training. The training must be made relevant to those receiving it, taking account of what they do and where in the world they do it.

A specific issue worth highlighting is the dubious legal status of what are sometimes called "facilitation payments". Under most legal systems, these small bribes paid to foreign officials to "speed up" service, are illegal and subject to prosecution. This causes real challenges for many international businesses. Frankly, it can be difficult to do business in some parts of the world without making such payments and head office disapproval may have little weight with agents, intermediaries and even remote employees.

The position is also complicated by the fact that some countries, including Australia, New Zealand, South Korea and the USA, allow facilitation payments when paid abroad, though they are illegal under domestic law.

The scale of the problem facing companies is illustrated by research from Berlin-based, Transparency International (*https://www.transparency.org*), which found that, globally, more than 1 in 4 people paid a bribe in a 12 months period. They reported that small bribes are "most likely to be demanded in overseas markets, where employees may be vulnerable through travelling alone or the company needs to release critical goods from customs".

Generally speaking anti-bribery law is not intended to prevent firms getting to know their clients better by taking them to events like a national tennis tournament or Grand Prix, but definitely strikes at "excessive" hospitality such as World Cup or Olympics tickets, supplemented by "spending money".

It is important to be aware of the "high risk" factor applicable to some countries. Statistically, the highest risk locations are countries suffering from wars or internal conflicts (for example, Somalia, Sudan, Libya and Afghanistan) or "rogue states" such as North Korea. These examples are places where it is unlikely that you will have mainstream relocation activity. But move down Transparency International's "corruption league table" just a little and you quickly come across countries where you may well have client activity. For example, if you have clients in the oil and gas sector, you may find that you have involvement with agents in countries which are designated "high-risk", such as Nigeria and Venezuela. What this means in practice is that, if you take the neighbouring countries of Finland ("low-risk") and Russia ("high-risk"), there is an obligation to carry out a higher level of due diligence on your new Russian supplier than on your new Finnish supplier.

In the context of international relocation, and by way of illustration, here is a current "top/bottom 10" based on Transparency International's latest research:

Ranking	LOWEST RISK	Ranking	HIGH RISK
1	Denmark	177	Venezuela
1	Finland	157	Zimbabwe
1	New Zealand	154	Nigeria
4	Norway	147	Mozambique
4	Singapore	140	Pakistan
4	Sweden	136	Russia
7	Switzerland	136	Angola
8	Netherlands	124	Mexico
9	Luxembourg	117	Egypt
10	Germany	117	Philipines

ISO publishes an international anti-bribery management system standard: ISO 37001. This voluntary standard is designed to assist organisations implement and maintain an effective and proportionate anti-bribery programme. Organisations can choose to use it simply as an internal benchmarking tool or seek ISO 37001 certification of their programme through an accredited agency.

Requirements in the standard include:

- An anti-bribery policy and procedures
- Commitment of top management
- Oversight by a compliance manager or similar function

- Anti-bribery training
- Risk assessments including appropriate due diligence
- Financial, procurement, contractual and commercial controls
- Monitoring and assurance processes around these controls
- Implementation of whistleblowing procedures
- Corrective action and on-going improvement

More detailed information is contained in Annex A to ISO 37001. This sets out the requirements to be met by organisations, along with guidance on how these can be met.

4. Relocation and Tax

Tax impacts on relocation businesses and relocation services in a wide variety of ways. Cross-border relocation, in particular, can give rise to complicated tax issues which require the input of tax professionals. So rather than attempting the impossible task of providing a comprehensive relocation tax guide, our goal here, instead, is to address two specific aspects of tax which most relocation businesses will encounter regularly:

a) VAT on invoices for relocation services
b) Tax on employee relocation packages

a) VAT

Within the relocation industry, we all work closely with our clients to ensure that unnecessary costs do not creep into the relocation process. VAT is a widely misunderstood tax which, if applied incorrectly, can give rise to just such unnecessary costs. Just as importantly, VAT compliance failures can lead to financial penalties and damage to reputation. It's important, therefore, for relocation professionals to have an understanding of at least the basics of VAT.

The Basics

EU and UK VAT is generally charged on supplies of goods and services made by businesses. Typically, businesses are able to reclaim VAT they are charged by other businesses, so it's only when a VAT charge is made to 'consumers' (i.e. those not in business) that VAT finally becomes a non-recoverable cost. The 'Value Added' part of Value Added Tax refers, therefore, to the various commercial stages and contractors that supplies can go through, before finally ending up being paid by the consumer. This multi-stage approach contrasts with other sales taxes, like in the US, which are simply taxes levied and collected on the final supply to consumers by retailers.

Different national rules and rates

While, in principle, VAT is designed to be a common system across all EU Member States, the rules can vary from country to country. The biggest differences relate to the application of VAT rates. All countries are able to choose to apply a standard rate and reduced rates but historically each has taken different routes when setting rates. That means, for example, that the UK has used a 'zero' VAT rate for things like public transport, books, foodstuffs and children's clothes, but charges 20% on hotels, whereas in, say Portugal, the VAT rate is 6% for both public transport and hotels.

Even where countries agree supplies should be charged at the Standard Rate of VAT, that rate can vary. The EU countries with the highest standard VAT rates are, currently, Hungary (27 percent), Croatia, Denmark, and Sweden (all at 25 percent). Luxembourg levies the lowest standard VAT rate at 16 percent, followed by Malta (18 percent), Cyprus, Germany, and Romania (all at 19 percent). The EU's average standard VAT rate is 21 percent, six percentage points higher than the minimum standard VAT rate required by EU regulation.

Is your service "land-related" or "General Rule"?

Deciding what rate of VAT applies to your services (which may often be supplied across borders) is one of the areas where a consistent rule applies across the EU. All EU Member States use the 'Place of Supply of Services' rules which apply to Business to Business (B2B) supplies. These rules should be applied by your company when deciding how and when to add VAT, by examining:

- where the supplier belongs;
- where the business customer belongs and
- the nature of the supplies made.

The starting point is called the "General Rule": the place of supply of services (and therefore the country where VAT is chargeable) is where the business customer belongs. That means that most B2B Supplies across EU Borders will not have VAT charged by the supplier, but the customer will 'self-account' in their own country through their VAT return (using what is known as the 'Reverse Charge' mechanism). Despite Brexit, this mechanism continues to apply to invoices issued by a UK business to an EU business and vice versa.

An important exception to the "General Rule" is "land-related" transactions. In the context of relocation services, the "land-related" exception is very important, because VAT on these services is due in the country where the land or property is situated. Examples of land-related supplies include:

- hotel accommodation;
- construction and repair/maintenance of any building
- services of estate agents, lawyers (including conveyancing) and surveyors where that relates to any specific apartment, house or piece of land.

In practice, this means that most relocation services, including the most common destination services, such as orientation, home search and settling-in support, will fall under the VAT "General Rule".

Applying the "General Rule" to your invoices

When considering the application of VAT to your invoices, it can be helpful to split your clients into three categories:

1) domestic clients
2) clients in other EU countries
3) clients based outside the EU

1) domestic clients
General Rule supplies made to an 'in-country' customer will be subject to local VAT at the prevailing rate in the country and accounted for by your business on your VAT return.

2) clients in other EU countries or UK
For B2B supplies to clients in other EU countries or UK, your client will self-account for VAT in their local country (using the Reverse Charge mechanism) and your business will not add any VAT (subject to obtaining your client's EU VAT registration number).

3) clients based outside the EU
Where a B2B supply is made to a client established outside the EU/UK, no EU VAT is due, as the supply is deemed to be outside the scope of EU/UK VAT.

Applying the "land-related" rules to your invoices

Taking the same three scenarios as above, but applying these to relocation services which are land-related (e.g. an estate agent's commission for a house sale or a lawyer's bill for vetting an expat's lease), local VAT is added to your invoice in each scenario, even where your client is established outside the EU.

What happens when several relocation services, with different VAT treatment, are being supplied?

It is not uncommon for a local relocation company to be providing a home search service ("general rule") and later vetting the tenancy agreement of the selected property ("land-related"). The issue then arises of whether your company can bundle the fees together or should you be issuing separate invoices?

This can be a real area of difficulty and is one of the aspects of VAT which is most frequently litigated in tax courts. In basic terms, there is a single supply and a single VAT liability when all the "supporting" or "incidental" services simply allow customers to "better enjoy" the main service. However, where each service is a means to its own end, then that is not a single supply but a "composite" supply and each aspect will have its own VAT liability according to the rules set out above.

So, the key question, where there are several services involved, is whether each service can be regarded as meeting a particular need ("composite" supply with each service separately taxed) or whether there is really a single supply with small supporting services enabling customers to better enjoy the main supply.

Each case can be different and its always advisable to consult local VAT specialists to ensure only the correctly due VAT is charged. This is particularly true in relation to instances where local VAT is to be reclaimed under the Refunds Schemes (see below), since all EU authorities will only repay VAT correctly incurred.

Claiming refunds of VAT

As outlined above, there are a number of circumstances where local VAT must be charged to businesses which do not have a local presence in that country (and are not registered for VAT in that country). If that VAT is incurred by way of business, it can be recovered using one of two refund mechanisms available:

1) If the business is established elsewhere in the EU ('home country'), using the EU Refund Scheme. This is an online system connected to the company VAT registration in their home country. Claims are made in the currency of the member state to whom the claim is made and that state should repay a valid claim within 4 months. In practice this may end up a far longer process.

2) For businesses established outside the EU, a paper-based reclaim can be made to the local EU Authority. Each country has its own detailed rules covering what can be claimed, deadlines and value of claims. You must claim your refund no later than six months after the end of the 'prescribed year' when you were charged the VAT. If you miss the deadline, you are unable to make a claim for that year.

What relocation costs are exempt from VAT?

The VAT treatment of relocation costs varies considerably. For example, in the UK, no VAT is charged on residential rent, but by contrast VAT is added to hotel bills.

Charging VAT and the rate of VAT applicable is a decision for each EU tax authority, often driven by a variety of conflicting drivers: social need, fiscal need and simple politics. Given the opportunity to apply different VAT rates, each EU country has done so. It is therefore vital that relocation businesses are fully aware of

local VAT rules, particularly around hotels and property rentals, and challenge suppliers where there is doubt.

Should you register your business for VAT in all countries where you deliver services?

In cross-border scenarios, it is very important to be clear as to who is supplying the end customer. Where that is the RMC, rather than its local supplier (e.g. DSP), it's likely that the RMC's supply can be treated under the General Rule and there is no need to register for VAT in the local country.

However, where an RMC has a physical or regular presence 'in country' and incurs sizeable local VAT, it may be sensible to register for local VAT. The advantage of that arrangement is the earlier recovery of local VAT incurred. The main downside means having to charge and account for local VAT on supplies as this can often mean an additional accounting resource, either within the RMC or outsourced.

If the arrangement is that local contractors act as principals and the RMC simply acts as 'middle-man', then no local supply is made by the RMC and there is no need to register for VAT. Any local VAT incurred in either case is reclaimable through the VAT refund schemes where the relocation company does not register for local VAT.

Follow the contracts ….. not the money!

An RMC will, typically, be providing services through its own network of approved suppliers, with no contractual relationship between a DSP and the ultimate corporate client.

However, in some cases, the RMC may be asked by the corporate client to work with a DSP who is contracting direct with the client. In this latter scenario, it is possible that the supplier's invoices may still be issued to the RMC for payment; and the RMC is simply arranging payment of costs that the corporate client has agreed to meet. These are, therefore, "disbursements" by the RMC and the supply subject to VAT is on the invoice from the DSP to the corporate client. This disbursement treatment requires that no uplift or profit is taken on that supply.

In terms of recovery of VAT in this situation, the corporate client will hold a VAT invoice to enable a reclaim, either through a local VAT registration or the local Refund Scheme.

Common VAT mistakes

There are three particular areas where businesses can easily hit VAT problems (resulting in unnecessary costs or a serious fall-out with the taxman):

- "VAT Blindness" – businesses ignore, are unaware or are just unwilling to focus on the VAT implications of proposed services. In practice it's far easier to ensure that VAT is not an irrecoverable cost when setting up your service delivery structure rather than seeking retrospective fixes or solutions after the event.

- Failing to get clarity on the "place of supply" of your supplies of services: where are you established, where is your customer and what is the nature of your supply?

- Failing to ensure that your suppliers and sub-contractors get their VAT decisions right. If VAT was correctly not due to be charged, local tax authorities will not refund it and the customer ends up with a VAT charge that is often "stranded" and irrecoverable.

It's clear that VAT produces a variety of challenges for the relocation industry, particularly for organisations operating across multiple EU countries. It is important for relocation businesses to have a decent grasp of the basics and to be alert to the situations where expert tax guidance is necessary.

It is worth noting that the European Commission is proposing far-reaching reform of the EU VAT system. A key objective is to simplify the tax system for businesses which have cross-border operations. The next stage in the legislative process requires lengthy consultations, involving all EU countries, so it is likely to be several years before the current system changes.

b) Tax on employee relocation packages

It is valuable for a relocation business to have at least a background understanding of how relocation support packages, including its own services, are treated for tax purposes. Across Europe, there is huge variety in the way that different countries impose tax on employees in receipt of relocation benefits.

For example, benefits provided to an employee, under a relocation policy, may be:

- Treated for income tax just like any other employee benefits in that country; and/or
- Taxed above a certain level (e.g. the UK has a tax free allowance of £8,000 for permitted relocation costs); and/or
- Fully taxable if paid as a lump-sum; and/or
- Taxable apart from certain categories of expenditure (e.g. only household goods removals may be reimbursed tax-free).

Tax treatment can vary in other ways. For example:

- Special tax rates may be applicable only to expats (e.g. The Netherlands);
- Foreign and domestic assignees may receive tax free accommodation for a limited, fixed period (e.g. UK assignments not due to exceed 2 years);
- Tax can vary according to whether a tenancy is taken in name of employer or employee (e.g. France).

Given this diversity of tax rules, from country to country, it is really not practical for most relocation businesses to keep up with basic tax rules beyond their own borders. But even in your own country, it is important to make clear to clients that any comments which you provide on tax are intended only as helpful pointers and that you are not providing tax advice. If a client has specific tax questions, they should always be referred to a tax professional.

Finally, there is one other aspect of expat tax which is much discussed in international HR departments. This is the difficult issue of which country's tax system (and social security system) is applicable to an expat assignment. By way of background, here is a summary of some of the main factors which can come into play:

- **First and last years of assignment:** the assignee is likely to be submitting tax returns in both the home and host countries. For this reason, it is very common for the employer to meet the cost of professional tax advice for the assignee, in both countries, in these two specific years.
- **Spending "too long" in a country:** good tax planning by an employer can be frustrated if an assignee spends longer than planned in a country, triggering unwelcome tax liabilities. As with

immigration rules, this is why there is a need to accurately track how long an assignee spends in a location.

- **Double taxation agreements:** these are agreements between two countries, which ensure that individuals do not pay tax twice on the same income. In the context of international assignments, these agreements can be very important. They specify which country has taxing rights over an individual, and, if they both have such rights, which one takes priority. They may also agree to exempt some income from tax or allow a set-off of tax paid in one country against tax due in the other.

- **Social security:** unlike national tax laws, the EU has specific rules in place to determine which country's social security system is applicable to an assignment. When an individual is sent on assignment to a different EU country, for up to 24 months, they remain in the home country social security system.

- **US citizens:** assignees who are US citizens never escape the US tax system! Their worldwide income always remains subject to US income tax, regardless of where in the world they are resident.

5. Insurance

Like businesses of all types, relocation firms face a variety of risks which can be protected against by using appropriate insurance cover. These risks may be based on your own assessment of "what can go wrong" or be a requirement of your clients or your professional body. Specific insurance cover, such as Employers' Liability, may also be a legal requirement in your country.

In practice, a relocation business will usually take out the following types of insurance:

1. Employers' Liability
2. Public Liability
3. Professional Indemnity (or Professional Liability)

1. Employers' liability

Once you take on your first employee, you may be required by law to take out employers' liability insurance. This will protect your employees if they fall ill or are injured in the course of their work. Your insurance certificate should be displayed where your staff can see it.

Even if you don't have any full-time employees, and just occasionally hire staff or use temps, you may be legally bound to take out cover. For example, in the UK you can be fined up to £2,500 per day if your business doesn't have a suitable employers' liability policy.

2. Public Liability

The law may not require you to have public liability insurance, but it's a cover that's crucial for businesses which come into contact with third parties. It is also insurance that is likely to be required by clients and professional bodies.

'Third party' includes your customers, your clients, your suppliers or any other member of the public who comes into contact with your business. The compensation amount will take into account things like medical bills, lost income and legal costs. Your public liability insurance would cover these costs, up to the limit of your policy. The policy limit should be at least sufficient to cover any amounts specified in your client contracts.

3. Professional Indemnity (also called "Professional Liability")

Professional indemnity (PI) insurance is a business essential for providers of all kinds of professional services, wishing to protect themselves from compensation claims from clients. Professional firms provide services

and advice upon which their clients depend. As a relocation professional, your skills are relied upon and sometimes, unavoidably, things can go wrong.

If you make a mistake during the course of your work, there is a possibility that it could cause some financial loss to your client and you may be held liable for any costs incurred as a result.

A good PI policy will protect you against the cost of the compensation claim itself, as well as helping to cover the cost of defending the claim. This might include legal fees, for which you would be held liable in the event that the client's complaint is upheld in court.

Even with insurance, it is of course preferable to avoid claims being made against you. Amongst the most important ways of preventing claims is to ensure that your contracts are watertight. Your arrangements with clients should be clear and unambiguous. Many claims can be avoided when both parties have a clear idea of what is expected of them.

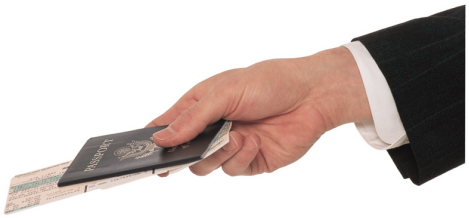
There is also a purely commercial element. Aside from good business practice and your own risk management considerations, there still remains the fact that RMCs and corporate clients are requiring their partners and suppliers to have PI cover in place. In this respect, PI insurance premiums simply become a necessary cost of being able to compete effectively for sizeable relocation contracts.
The Risk Management section of the EGQS Standard states:
"A professional liability insurance policy that covers company's operations on as near a global basis as possible, beyond the borders of the home country and most importantly in the United States would reduce the financial risks enormously".

With growing attention being paid to various forms of cyber-crime, including deliberate hacking and potential ransom demands, it is important to have clarity from your insurance broker on the cyber risks which are covered by your PI policy. Do you have gaps in your insurance coverage that may need to be covered by additional cyber insurance?

6. Cross-border employment and start-up issues

Employing staff in a different country - basic rules

Employers often mistakenly think that employment regulations are similar across Europe. It is also common to find companies, headquartered outside the Europe, using standard employment documents based on their national laws when drafting contracts for European employees. These misconceptions can result in basic mistakes in the wording of clauses for the termination of employment, non-compete clauses and other important employment terms.



Employment is one area of law where European harmonisation is very limited. So, if you expand your business into a new country, it is critical that you obtain professional advice on that country's start-up and employment laws before you commence business. Even in countries where red tape is relatively light, you will be faced with a range of compliance requirements, which typically will include:

- Recruitment - check that each of your new employees has the legal right to work in that country
- Employee background checks - most EU countries have strict rules around what checks an employer is permitted to carry out. Breaching these rules can be a criminal offence.
- Salary - you must pay your employee at least the National Minimum Wage
- Insurance - you need employers' liability insurance as soon as you become an employer. You can be fined if you are not properly insured in accordance with local law.
- Statement of employment - you will probably need to send details of the job (including terms and conditions) in writing to each employee, within a fixed timescale (e.g. thirty days).
- Register as an employer - with the national tax authority and, in some countries, you may also need to register your business with the local chamber of commerce.

Employment protection in Europe

By international standards, European countries provide strong legal protection to employees and regulate many aspects of the employer/employee relationship. An illustration of this, which can surprise US-headquartered businesses, is that the common US practice of "employment-at-will" cannot be applied in Europe. Once an employee's probationary period is completed, European employment laws invariably require mandatory notice periods to be given to the employee prior to termination of employment.

In addition, after a fixed period (e.g. 12 or 24 months), European employees acquire legal protection against "unfair dismissal". This means an employer only terminates an employee's job lawfully if the employer follows a fair procedure, acts reasonably and has a valid reason.

Which law applies?

In the context of international assignments, there can sometimes be difficulty in establishing whether the assignee is protected by employment law in the host country or if the employment relationship continues to fall under the employment law of the home country. While this should be stated explicitly in the letter of assignment, it is still possible that the assignee will acquire host country protection after a certain period.

Even where two EU countries are involved, there can be challenges in establishing which country's employment law should apply. This issue went to the European Court of Justice (ECJ), in 2013, in the case of Schlecker v Boedeker.

Ms Boedeker worked for many years for a German company (Schleker), with branches in several EU countries. Latterly, she was based in the Netherlands and, in a dispute with her employer, she raised a legal action under Dutch law, which happened to be more favourable to her case than German law. However, the ECJ ruled that there had to be an objective assessment of which country was more closely associated with the job and not simply a selection made by the employee. This assessment should take account of the country in which the employee pays taxes on the income from her activity and the country in which she is covered by a social security scheme and pension, sickness insurance and invalidity schemes.

In a similar case (Fuller v United Healthcare Inc), a UK court had to decide whether UK employment law should apply to a dismissal of an American employee.

Mr Fuller, a US citizen, was employed by a US company and paid in dollars. He was given responsibility for overseeing the UK and Abu Dhabi businesses and spent around half his time in the UK. When the company decided to appoint a local hire to head up the UK business, Mr Fuller had his secondment terminated and later he was made redundant. He raised an unfair dismissal action in the UK, claiming that his dismissal was motivated by his sexuality and whistleblowing.

The UK court decided that Mr Fuller fell outside the territorial scope of UK employment law. Despite carrying out work in the UK and other countries, he had not given up his base in the US and his employment contract had an "overwhelmingly close connection" with the US. It was also a factor that his dismissal had taken place in the US after his UK assignment had come to an end. In summary, Mr Fuller did not have the required connection with the UK for him to be protected by UK employment law.

Employee monitoring versus employee privacy

As an employer, do you have the right to monitor your employees' communications at work, or do your employees have the right to privacy?

This is an issue which is becoming more common as businesses rely on an increasing variety of methods of electronic communication to carry out daily work. E-mails, Internet, text messages, personal messenger are all common methods of communication in the workplace and with that comes a temptation to blur the lines between business and personal use during working time.

The European Court of Human Rights (ECHR) considered this in the case of Barbulescu v Romania. Mr Barbulescu was an engineer who used his work-related Yahoo Messenger account to send and receive personal messages with his fiancée and his brother, including messages about his health and sex life. This was in breach of his employment contract and his employer's IT policy. His employer discovered this accidentally and dismissed him as a result. Mr Barbulescu argued that all evidence of his personal communications should have been excluded on the grounds that it infringed his right to privacy.

The ECHR ruled that the employee's privacy rights had been infringed as a result of his employer's decision to monitor personal messages. A key factor in the ruling was that the employee had not been informed of the nature and extent of the monitoring or of the possibility that the employer may access the actual content of messages. The Romanian courts had failed to strike a fair balance between the relevant competing interests and had not adequately protected the employee's right to respect for his private life and correspondence. However, this was very much a technical victory for the employee, as the court dismissed his claim for damages.

The Barbulescu case has been followed recently by another important ECHR decision, in the 2019 case of Lopez Ribalda v Spain. This involved an employer's use of covert CCTV surveillance of staff in a supermarket following concerns about the amount of stock that was going missing. Goods valued at over €82,000 had been taken over a five month period before the employer set up video surveillance. The surveillance was set up for ten days and provided evidence of theft. As a result, several employees were dismissed.

Some of the employees raised court action against their ex-employer, arguing that their right of privacy had been breached and also that Spanish data protection law, which requires individuals to be informed about CCTV use, had been breached. The Court decided that the employer had a legitimate reason (suspicion of serious theft) to implement the surveillance and took into account that the surveillance continued only until the culprits were identified. Despite deciding in favour of the employer in this case, the Court made it clear that, *generally speaking,* the slightest suspicion of wrongdoing would not usually justify covert video surveillance.

Germany and Finland probably have the strictest laws regulating the manual or electronic surveillance of employees' computer usage and email communications. In Germany, monitoring is strictly forbidden if the employee is allowed personal use of company equipment. In other European countries, the monitoring of work-related emails is generally permissible but the interrogation of private emails is strictly prohibited.

What should a business do … and not do?

- Review what policies, if any, are in place to support the need for reasonable and proportionate monitoring of personal communications.

- Have in place an appropriate IT and electronic systems policy, together with a social media policy. Employee use of social networking or blogging sites is conduct which usually takes place outside work, however this may have a bearing on the reputation of the business in the event, for example, that derogatory remarks are made about the business.

- Ensure that HR policies are clear and use transparent wording. Most employers tolerate at least some personal Internet and telephone use at work and it is important that the parameters of such use are set out and clear.

- Ensure that the policies highlight the right for employers to monitor employees' use of electronic communications and systems in the workplace and also highlight the sanctions applicable for breach of such policy.

- Consider if existing policies are sufficiently clear as to any CCTV surveillance which may take place within the workplace.

- Ensure that the policies are applied consistently and fairly to avoid claims for unfair dismissal and discrimination. For example, if the policy states that offensive jokes and images should not be circulated in the workplace, but then permits some employees to send jokes or images, singling out an employee for dismissal on this basis is likely to be unfair.

If you suspect an employee of misuse of electronic communications or misconduct relating to social media, it is important to carry out a full investigation to substantiate the suspicion and gather all available evidence.

Can you prevent an employee from moving to a competitor?

A "restrictive covenant" is a clause in an employment contract, which seeks to regulate an employee's ability to compete with the former employer after the employment has ended. As a matter of public policy, these clauses are void in some parts of the world, including for example, India, Russia and the State of California. However, in Europe, these clauses are enforceable provided that there is a legitimate business interest to protect and that the restraints are reasonable (e.g. in terms of the duration of the restriction).

Many European companies impose restrictions relating to:

- Working for a competitor
- Contacting customers
- Poaching former colleagues

Typical restraint periods are one year for most European countries, up to two years in Germany and Turkey, up to three years in Switzerland and three to five years in Italy. In many EU countries, the restriction is only legally enforceable if the employee has received compensation to "stay out of the game". This payment is typically around 50% of gross salary. No such payment is required in the Netherlands or the UK.

7. Expat Tenancies

Tenancy law and all the related tenancy practices and processes are unique to each country in Europe. While corporate clients will seek as much global consistency as possible, it is important that relocation professionals can explain local practical realities and are able to offer alternative solutions.

The specific challenges vary from country to country, but will typically include:

- Health and safety issues
- Break clauses and options to renew
- Ensuring that landlords and agents meet their obligations
- Recovery of security deposits (and handling dilapidation claims)

A particular issue on which corporate clients often need guidance is the question of whether it is better to have a Tenancy Agreement put in the name of the client or in the name of the assignee. This can be a complicated issue and can sometimes give rise to challenges for a relocation adviser who is trying to give best advice to their client. The starting point will often be the employer's global policy, which could be "we always take the lease in our corporate name" - or may be the exact opposite: "the lease must be taken in the employee's name"!

But a strict global policy on this issue may result in unnecessary costs or complications, which arise from the laws, tax rules and common practices of individual countries.

Based on input from EuRA members, below is a snapshot of what is currently common practice in a variety of European countries. This overview is for background information only and should not be relied upon when giving advice to clients.

Belgium

A tenancy contract in the name of a company, rather than an individual tenant is viewed by the taxation authorities as a commercial lease rather than a residential agreement, resulting in significantly higher taxation implications for the Landlord. Consequently, clients requiring a corporate lease are usually restricted to seeking properties owned by companies, rather than by private individuals, to avoid the significant fiscal penalty which would otherwise arise for the Landlord. The number of houses/apartments for private occupation, belonging to a company, is very limited

For corporate/furnished housing, business flats for stays of 3 to 6 months, the lease agreement is always regarded as a commercial lease.

Bulgaria (Sofia)

From a legal perspective there is no difference whether a personal and corporate lease is signed but there are some tax issues to be taken into consideration:

- If both the tenant and the landlord are companies then VAT is charged and potentially the tenant will be able to claim it back. VAT in Bulgaria is currently 20 %.

- If the tenant is a company but the landlord is an individual then the tenant is obliged to deduct and pay directly to the tax authorities the due tax on the rental income and transfer to the landlord just the remaining part. So in such cases the landlords would prefer individuals as tenants to try and avoid this tax payment.

- If the tenant is an individual but the landlord is a company, the landlord would in most cases need to charge VAT on top of the rent which means higher rent for the tenant since they will not be able to claim it from the tax authorities. However, VAT law allows some exceptions to this rule that may help avoiding VAT payment by both parties.

- If both the tenant and landlord are individuals then it would be a matter of negotiations between them how the payments will be arranged (by bank or cash) and what taxes will be paid.

In Bulgaria, as in most EU countries, at the moment the market is extremely dynamic. Whoever pays first has some advantage but even this is not a sure thing anymore because often there are 2 or 3 more people who have also agreed to pay cash on the spot. So the Landlord has to choose whose money to take. If the rental agreement will be signed by a company as a tenant, this may slightly delay the process but in general if the company policy is clear and structured this does not take too long to process and will not put the signing of the agreement at risk.

In any case landlords generally feel more secure if the rental agreement is signed with a company or if the tenant works for a big multinational company.

Czech Republic (Prague)

From a legal perspective, if the tenant is a private individual, they are quite well protected by the civil code. In the case of a corporate lease, the rights and obligations for both parties are more balanced and the protection provided to the tenant very much depends on what is stipulated in the lease contract.

Most landlords do not have a particular preference for a personal or corporate tenancy. From the perspective of a DSP, getting a corporate lease approved takes much more time and from this perspective a personal lease is easier and quicker to complete and to allow the tenant to move in. In general, we see a trend towards personal rather than corporate leases. This appears to be driven by employers more commonly requiring that their foreign assignees "take care of themselves".

Denmark

Legally, corporate and personal leases in Denmark are the same. Corporate leases are considered more attractive by landlords / agencies for their perceived financial security. The company signatory must be listed in public company records as authorized to sign. In rare instances, a corporate lease is the only accepted type of lease.

With corporate leases it is important to ensure clear distinction between lessee (signatory) and occupant. The occupant's rights and responsibilities should be clearly defined in the lease contract and the assignee should be clearly listed as 'occupant' for purposes of municipal registration.

Diplomatic clauses are generally requested on both corporate and personal leases. However, in our current real estate market, the landlords/agents dictate the lease terms. For example, 9 month's locked with a 3 month termination notice. Or 12 months locked with 3 months termination.

An additional factor now is that more leases include a price index increase annually. There is a designated spot for this in the lease agreement. In **rare** circumstances, this is a negotiable term.

Estate agent fees are paid by the Landlord to the rental agency.

Third party payment of rent from abroad (i.e. from RMC) requires legal paperwork. It has proven to be challenging to get Danish landlords to complete this requirement.

Estonia (Tallinn)

There is generally not much of a preference for the landlord in Estonia as to whether the lease is corporate or private. If the property is rented for residential purposes, then there is no tax difference between having a company or private individual as the lessee. Sometimes agreeing terms on a corporate lease is more time-consuming, so in matters where speed is essential a private lease is preferred to get everything over the line before the deadline.

Finland

Corporate and personal leases in Finland are legally the same and pursuant to the comprehensive rights and protections laid out in the Act on Residential Leases. Guidelines for conduct are also set in Fair Rental Practices, which is published jointly by major landlord and tenant organizations.

Landlords do not have a set preference whether the lease is corporate or private. Agents are allowed to charge a commission from corporate lessees, but not from private ones. Minimum tenancy of 1 year is typical, for both corporate and private leases. Deposits are legally limited to 3 times monthly rent, but 1-2 months is the norm. Although not strictly regulated, deposits should be returned within 2 weeks after the end of lease.

Employer-provided accommodation is treated as a taxable accommodation benefit. The taxable value of the apartment depends on its age, area, and any improvements it may have had. In addition, the taxable value of apartments in the Helsinki area is higher than elsewhere in Finland. The taxable value of accommodation determined by the Finnish Tax Administration consists of a monthly basic value and an additional value per square metre. Deductions are made for certain situations, such as if the employee is using the apartment for employer's entertainment events.

The calculation formula may result in a substantial tax benefit compared to renting the apartment directly. This is especially the case for furnished high-end housing in expensive neighbourhoods or short term furnished apartments.

France

We are seeing more and more companies favouring personal leases for their transferees. For personal leases, the tenancy acceptance process in France is substantial. The transferee needs to have a strong service reference with his/her employer (hence not be in a new hire or trial period situation) and have a total monthly compensation net (housing allowance included as applicable) to correspond to 3 to 4 times the total monthly rent amount. Even when these 2 main criteria are met, ad hoc guarantees in the form of a bank guarantee or 3rd party guarantee may be requested. A bank guarantee does imply blocking one year's worth of rent in an escrow account in France for the duration of the occupancy.

A corporate lease, in the French entity's name, avoids these requirements, as the property owner will be looking at the financial standing of a French company. The transferee's name appears as the occupant and there are tax advantages with a corporate lease when the transferee benefits from an expat package and housing allowance.

Note: with the upcoming Olympic Games in France from July – Sept. 2024, the candidacy acceptance process for individual leases has become stringent, with tenancy profiles and documentation being required before a viewing may be granted.

Germany

In Germany there is no difference between a corporate and personal tenancy from the tax and the legal perspective. However, more and more clients opt for a personal tenancy and monthly rent allowances because it is believed that employees then take much better care of the properties. Also, when the tenancy agreement needs a diplomatic or break clause, allowing termination of the lease prior to the agreed duration, this only applies to personal leases and not to corporate leases.

Besides that, when US companies pay rents to German landlords this requires a W8N confirmation from the landlord to allow third country payment. Most German landlords are reluctant to sign such an unfamiliar document, especially outside the major cities.

More and more landlords insist on a minimum tenancy of 2 years.

Hungary (Budapest)

In legal terms there is no practical difference between a personal and corporate lease; the housing law applies in both cases. From a tax perspective there are a couple of potential minor issues. If the owner of a property is a legal entity then there is sometimes, but not always, a requirement to charge VAT on top of the rent. With a corporate lease the tenant may be required to withhold the tax payable on the landlord's income and pay it direct to the tax authority.

As the lower end of the housing market in Budapest (generally rents of less than 1,000 EUR/month) is currently extremely dynamic, the ability to make a swift decision and even pay a cash deposit on the spot is more and more important. The requirement for a cumbersome lease approval process can put deals at risk as landlords will generally choose to conclude a deal quickly if they can choose to do so. In general terms, for lower budget properties a personal lease is preferable and for a higher budget property the perceived security of a corporate lease is seen as an advantage.

In 2024, the mid to high end of the housing market (2,000 - 5,000 EUR/month) is also becoming challenging for potential tenants. The supply of suitable quality properties is very limited, there is plenty of demand and landlords are less flexible in terms of lease negotiation. Over the course of the last year rents increased significantly due to strong increase in demand and in parallel significant decrease in supply across the market.

Ireland

The trend is moving from corporate leases to personal leases. The main reasons for this are:

1) The name of the occupier is usually requested by the landlord

2) The lease can be used as proof of address when applying for a Social Security No. (called PPS No. in Ireland)
3) Companies are not held responsible for any dilapidations when the lease is in the assignee's name.

It is worth highlighting that agents will require proof of salary on the employment reference and many agents require that the rent is less than 40% of the assignee's net salary.

Latvia (Riga)

Many landlords in Latvia still prefer to work directly with the tenant when signing a lease. This gives them more flexibility in deciding how to handle the issue of taxation. If a lease is signed with a company, the company is obligated to ensure that a tax of either 10% or 15% is paid by the landlord. In some cases, the company insists on having proof that this tax is being paid by the landlord, so that it does not become a liability for the company. This tends to complicate the process for some landlords and they may then prefer to rent directly to a private person. Companies can write off the tax in most cases but tend to be flexible on who is signing the lease and being responsible for making the rent payments. Adding to this, a company must pay 21% VAT if the landlord is also a company.

Personal leases are preferable in Latvia as it simplifies the lease-signing process. In most cases, landlords will still feel that a reputable employer is behind the tenant, so there is a sense of security in terms of the tenant paying their rent.

Luxembourg

In Luxembourg property owners prefer corporate over personal tenancies, as it reduces the risks for the owner. There is no difference in legal protection, but corporate tenancies have less chance of rent arrears. Furthermore, in Luxembourg, an agency fee has to be paid to the real estate agent and a company is able to reclaim the VAT on that fee. On the other hand, most companies do not want to take on corporate leases, as they will have to carry the risks of assignees who breach the lease terms.

The diplomatic clause will have to be amended and negotiated to be linked to the occupant and not the tenant.

Netherlands

Corporate leases for long term rental properties are usually only for high level employees, where the rent is paid by the corporate. While corporate leases still exist, there are more and more personal tenancies. For personal rental agreements, an owner is asking for both a work contract from the prospective tenant, a copy of the passport, and often also an employer statement. Even for high rents, paid for by the company, a lease is nowadays often in the name of the employee. The employee gets an allowance from the corporate to pay the rent, so the tenant pays the owner directly.

The only tax advantage of a corporate lease is that VAT can be reclaimed on the agency fee. Usually the fee is 1 month's rent plus VAT (21% in 2024).

Corporate leases require specific documentation, including a recent extract from the Chamber of Commerce registration, identification of the person who will sign the lease and a power of attorney from the company (unless the signatory is specified in the Chamber of Commerce registration). Most homeowners will not accept a company lease anymore.

Poland (Warsaw)

There are no differences in legal terms between a corporate and private lease. Corporate leases are sometimes preferred by property owners as offering greater financial security. Frequently, however, landlords are more willing to come to an agreement with an individual, and are reluctant to sign a corporate contract because of perceived greater commitment and fear of dealing with a very large institution.

This is especially true when companies request the use of contracts they prepared, which are usually much longer and constricting than regular lease agreements. When a standard contract can be used, most landlords are indifferent as to whether they sign a contract with an individual, or with a company.

Corporate leases also face a recurring issue in the current real estate market, which is the need to be able to start renting very quickly. Companies often require many working days to process and approve the contract, internally schedule payments etc. In the current market, a tenant has to be able to start paying rent no more than two to three days after selecting an apartment, otherwise the owners will very often choose a more agile tenant.

Portugal

Landlords prefer the lease to be in name of the individual tenant, with the company as guarantor. If no guarantor is available some landlords may not be prepared to rent; others may be willing to waive the guarantor in exchange for an extra security deposit.

If the tenant is the company: utilities should be in the name of the company and the name and ID of the Tenant should be mentioned in the lease as resident.

Monthly rent is always paid in advance.

A Diplomatic Clause is not provided by law. Early terminations are possible, but the tenant needs to comply with a minimum period, corresponding to one third of the lease duration, plus applicable pre-notice period.

Real Estate commission is paid by the landlord.

Romania (Bucharest)

Both options are applicable for the local rental market, each having its advantages and disadvantages:

Personal rental contracts: the landlords can be more reluctant to rent to a private person, but this is strongly influenced by budget level, as after a certain level their reluctance slowly dissipates. Also, some properties that are owned by companies may have VAT (19%) added on top of the rent and as a private person you are unable to deduct or claim back the VAT, in other words, you must add another 19% on top of the rental price and pay that amount. On the other hand, the lease contract negotiations, signing, and payments are much faster and this constitutes a real advantage, especially for properties that are targeted by lower rental budgets (typically those below 800 EUR/month). For this category of properties sometimes the decision and even a deposit needs to be made or paid on the spot.

Corporate rental contract: the landlord would prefer signing a contract with a company as tenant, as this offers more perceived financial security. Nevertheless, for those properties where VAT is added on top of

the rent, some companies have the possibility to deduct the VAT, thus it offers the assignee a wider range of properties from which to choose within the budget limits. On the downside, the lease contract negotiations and signing can be prolonged, require more documentation from the owner and the payment terms can be far worse than the common rental practice in Romania. Last, but not least, for the corporate leases we might have a third party involved (e.g. an RMC) making the rent and deposit payments and the owners and the banks might ask for proof of contractual relationship between parties as justification for the bank transfers. In short, corporate contracts are more strict, can lead to deal breakdown but offer more security on the long run.

The ideal situation would be a personal rental contract and for the company to provide the assignee with a rental budget that would cover also the VAT, if this is applicable. We have seen this model applied by a large corporation that preferred to move all corporate contracts to personal ones, but in order not to deprive the assignees from visiting properties that together with VAT would have exceeded the budget, they have agreed to assume also the cost of the VAT.

Note: based on the new local fiscal laws, a corporate lease made with an individual person landlord has become a bit complicated, as the tenant will have to pay the taxes that result from the rental income directly to the state, as this no longer falls under owner responsibility. The value of the rent will remain the same in the rental contract, but the tenant (the company) will deduct the value of the taxes (8% from the value of the rent), transfer the remaining amount as rent to the landlord and the taxes directly to the fiscal authorities. For examples: rent contract concluded between landlord natural person and the tenant, juridical company, for a rent of 1000 EUR mentioned in the rental contract. The Tenant will transfer 920 EUR as rent to the landlord and 80 EUR taxes to the state.

Slovakia

Companies in Slovakia have various policies in relation to signing leases on behalf of their relocating employees.

In the last decade we have seen a trend that companies tend to transfer responsibility for the lease signing to the assignee. Top management positions remain the ones that receive support from the company, with the lease being arranged in the company’s instead of the assignee's name.

Leases where the company acts as tenant and the assignee is just the occupant of the property are more time-consuming to negotiate. The company requires more information from the Landlord including Tax Registration Certificates, proof of bank account ownership and the process is often delayed by the need for the company to enrol the Landlord into some kind of system as a new vendor. Lease preparation, including the gathering of supporting documentation, lease negotiation as well as arrangement of the first payments of deposit, rent or any related fees are impacted by these processes.

A new challenge is arising in Slovakia where the lease is signed by the assignee but the deposit, rent or sometimes both are transferred by a third party. Landlords, especially those who own the property as a legal entity, are requesting proof of the relationship between the parties and clarification as to why the funds are being transferred by a party that is not mentioned in the contract; sometimes raising concerns of unlawful enrichment. The same standards of transparency and a clear paper trail are being demanded by Slovak landlords and their accountants.

Slovenia (Ljubljana)

In general, Slovenian landlords don't really have a preference between renting to an individual who has a steady job at a company in good standing or a corporation, if the landlord has a sense of security in terms of payments being made in a timely manner. Generally landlords prefer longer leases and in this case it is likely that they will be willing to negotiate a lower rent, be it with a corporate tenant or with an individual. This said, there are still some landlords who prefer to get paid at least partly in cash and these will obviously prefer renting to private individuals.

Spain

This is a complex question as it depends how the property is set up for tax purposes. The law is quite complicated.

For example, if the owners have registered the property in the name of a company and it is a corporate lease, then tax will be applied. In principle this is 21% unless it is registered as a short-term apartment and the rate is then reduced to 10%. If the landlord is an individual and the tenant is a company, and the company requires a monthly invoice for processing payments then VAT is applied. Individual landlords can be reluctant to issue an invoice due to the taxation and bureaucratic consequences. If the tenant is an individual and the property is also owned by an individual, then tax is not usually applied.

When it is a corporate signing, the company will often be asked to produce the power of attorney of the person signing on behalf of the company, along with ID and other company documents. Quite a lot of documentation needs to be presented, which can be particularly challenging for an overseas company.

In summary, the law is a little "grey" and it depends entirely on the circumstances of each situation and how the property is registered. In practice, we find that the majority of cases are personal leases.

Sweden

Housing market for expats are regulated based on the property type.

For houses or apartments owned by tenancy associations (referred to as Bostadsrätter BRF), there is distinct legislation as part of the Swedish Tenancy Act that applies. Landlords retain the flexibility to set their own rental rates within liberal legislation but it also gives the tenant a shorter notice time (1 month). Furthermore, both parties have the option to terminate the rental agreement prematurely.

However, subletting rental apartments follows stricter guidelines. Landlords are subject to regulated rental rates and tenants have a longer notice period (3 months). Additionally, landlords are obligated to keep to the original lease duration.

Both BRF's and rental apartments are bound to legal limitations of subletting for a maximum of 2-3 years. To be allowed to sublet your apartment the owner, or 1st hand lease holder, must provide a legal reason to sublet and obtain approval from the real estate owner or tenancy association. House sublets are not exposed to this requirement.

For the purposes of obtaining a Swedish bank account, the name of the occupant (assignee) must be visible on the lease.

In cases of dispute resolution, the Tenancy Act applies.

The private market for rental accommodation is limited in all of Sweden. Corporate signing is often considered as a security for landlords but many BRF's do not permit a company as tenant. First-hand rental leases are very difficult to get in the major cities.

Corporate services apartments are often available in the urban areas – these require corporate signing.

United Kingdom

There is no difference in the tax treatment of corporate and personal tenancies. There is, however, greater legal protection for personal leases, as these are protected by deposit protection rules and consumer "unfair contract" legislation. Overall, the general trend is a move away from corporate to personal leases, though many US employers retain a preference for corporate leases.

Thanks are due to the following EuRA members who have contributed to this overview of expat tenancies: Altair Global, Antares Relocation, Copenhagen Relocations, European Relocation Services SA, Executive Relocations, Inter Relocation, Key Relocation, Locators, Moving-ON and Palladium Mobility Group.

We encourage EuRA members to continue to share with us their experience of tenancy "best practice" in their locations.

8. Other Legal Issues

a) Anti-Money Laundering

Anti-Money Laundering ("AML") laws are intended to ensure that businesses at risk of being used for money laundering have controls in place to minimise the risk of this happening. Across Europe there are a myriad of laws, regulations, policies, procedures, guidance and recommendations. In many countries, it is an offence to provide relocation services unless you are registered with the national authority responsible for anti-money laundering supervision (e.g. HMRC in the UK).

EU regulation of this area is contained in a series of Directives, the most recent one being the 5th Directive, adopted in 2018. Because EU law on money laundering is in the form of Directives, rather than Regulations, compliance rules vary between countries.

The starting point for any business is to seek clarity about what AML regulations are applicable, including any requirement to formally register your business. For example, if you occasionally provide a home search service for property buyers or marketing assistance for sellers, then these services are likely to trigger a requirement to register your business and to comply with the specific AML rules applicable to estate agency services.

Even where your DSP work is limited to home search for renters, there may be a requirement to register your business for AML purposes if the monthly rent exceeds a certain level (e.g. €10,000 in the UK).

AML rules require your business to put in place certain controls to prevent your business from being used for money laundering. Typically, these controls will include:

- assessing the risk of your business being used by criminals to launder money
- checking the identity of your clients
- checking the identity of 'beneficial owners' of corporate clients and partnerships
- reporting anything suspicious about your clients' business activities
- making sure you have the necessary management control systems in place
- keeping all documents that relate to financial transactions, the identity of your customers, risk assessment and management procedures and processes
- making sure that your staff receive money laundering training.

Your national supervising authority will be entitled to audit your AML processes. Typically, the starting point you will be a written request for you to provide the following documents:

- AML Risk Assessment
- AML Policies, Controls and Procedures
- AML Training Log

An unsatisfactory audit may trigger a civil penalty or criminal prosecution, so this is not an area of compliance which you can afford to neglect.

b) Competition Law

Competition law is usually associated with unlawful activities of large corporations which may, for example, be conspiring together to obtain higher prices from their customers. But competition law is applicable to businesses of all size. Relocation businesses, which can often be involved in legitimate co-operation with competitors, must be careful to avoid crossing the line from legal to illegal sharing of information.

An example of anti-competitive behaviour in the estate agency world is where a group of estate agents in a locality agree to establish a minimum rate of commission for their services. Such an agreement, however informal, is likely to attract substantial fines for all the businesses involved.

The setting of an industry conference, where competitors mix in a convivial atmosphere, is also where innocent conversations can easily cross a line into illegality. That is why Worldwide ERC, for example, has a written policy which states that:

"*Members of the association should avoid discussing matters involving price or pricing policy, terms and conditions of sale, the allocation of territories or customers, bid rigging or any other subjects that would restrain competition or raise antitrust issues*".

While these forms of anti-competitive behavior can result in corporate fines - and several international moving companies have in the past suffered large fines at the hands of the EU Commission - there is also the risk of individual prosecution and imprisonment for terms of up to ten years.

Most anti-competitive behavior is obvious and indefensible, but where relocation companies can accidentally stumble into legal problems is where a legitimate discussion of a common industry problem develops into agreement to take "collective action" in the marketplace. At this stage a red warning light should come on and it's time to withdraw from the discussion!

If you suspect that your business is becoming enmeshed in any form of anti-competitive behavior, there is an incentive to report this to your national authority. Fines will usually be significantly reduced for companies which "blow the whistle" on unlawful activities.

9. Legal Compliance and the EuRA Global Quality Seal+

Highlighted below are the specific areas where legal compliance is a stated requirement of EGQS accreditation. Numbered references below refer to clauses in the Global Quality Seal Standard Plus 2022 ("the Standard").

- **Compliance Management (2.2)**

A key part of "Compliance Management" is the requirement that *"knowledge and application of valid rules and regulations are developed and implemented, appropriate for the purpose of the organisation, ensuring compliance with local and international law*".

For this purpose, your company should have in place "*a list with all relevant and applicable country-specific laws and regulations or EU guidelines i.e., data privacy or money laundering regulations, regulations/laws covering VAT, immigration, tenancy, and health and safety.*"

- **Anti-Corruption/Anti-Fraud Policy (2.6)**

The Standard requires companies to have an up-to-date Anti-Corruption/Anti-Fraud Policy, which:

- "*Is developed and implemented appropriate to the purpose of the organisation and is in compliance with local and international law.*
- *Is documented, communicated and understood within the organisation.*
- *Is reviewed at least one time a year during the management review*".

- **Data Protection, Integrity and Information Security Policy (2.9)**

The Standard requires companies to maintain a policy which is compliant with:

- "*EU GDPR on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, if applicable.*
- *Is documented, communicated and understood within the organisation.*
- *Is reviewed at least one time a year during the management review*".

- **Information Security and Data Protection (2.14)**

The Standard requires compliance with the GDPR and specifies a range of detailed requirements.

With reference to the risk of data privacy breaches, the recommendation in the Standard is that:
"It is advisable that the company maintains not less than $500,000 of cyber risk insurance for operations on as near a global basis as possible, beyond the borders of the home country and most importantly in the United States, to respond to privacy and data breach/unauthorized access liability claims".

- **Outsourced Processes (3.5)**

If any services are outsourced, the Standard requires companies to enter contracts with such suppliers.

"If an organisation chooses to outsource any process or service that affects the service quality, the organisation shall ensure control over such processes.

Minimum requirements, e.g. proven competence in the job/process, for partners and suppliers are determined and documented in a contract and/or agreement according to relevant local, EU and international law. Part of the contract/agreement shall be that the partner/supplier is not allowed to
subcontract another person to deliver the agreed services without a written permission by the company."

- **Service Contract (4.1)**

The Standard requires that relocation services to be delivered are agreed upon with the client or customer in advance and in writing.

Glossary of Terms

Arbitration: an alternative to court action which involves the parties to a dispute agreeing to appoint an independent arbiter who will assess the evidence and make a decision. An arbitration process should be cheaper and faster than going through the courts.

Break clause: a clause in a Lease or Tenancy Agreement which allows the Tenant to terminate the lease early, on the occurrence of specified events, such as the termination of the Tenant's current assignment. A "mutual break clause" is one which also allows the Landlord to terminate early.

Class action: a court case raised by a group of individuals which is based on a collective grievance.

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.

Corporate lease: a Lease or Tenancy Agreement where the Tenant is the corporate employer (rather than the individual Assignee).

Directive: EU legislation which sets out a policy goal, but only becomes law when it is followed up by legislation at a national level, by each EU member state..

EGQS: EuRA Global Quality Seal - a quality accreditation for relocation businesses.

European Commission: the EU institution responsible for proposing legislation, implementing decisions, upholding EU treaties and managing the day-to-day business of the EU.

European Court of Justice (ECJ): the highest court in the EU, responsible for interpreting EU law and ensuring its application across all EU member states.

European Court of Human Rights (ECHR): an international court established by the European Convention on Human Rights. It hears applications alleging that a country has breached one or more of the human rights provisions set out in the Convention. The ECHR is not an EU institution.

European Economic Area (EEA): EU member states, plus Iceland, Liechtenstein and Norway.

General Data Protection Regulation (GDPR): EU-wide data protection law, which came into force on 25th May 2018.

Indemnity clause: a clause in a contract which makes one party responsible for compensating the other party for losses incurred as a result of certain specified events.

Jurisdiction: the territory over which the legal authority of a court extends.

Letter of Assignment: a document setting out the amended terms of employment which will apply while an employee is on international (or domestic) assignment.

Money laundering: the process by which criminals disguise the original ownership and control of the proceeds of crime by taking steps which have the affect of making funds appear to have come from a legitimate source.

Option to renew: a clause in a Lease or Tenancy Agreement, which allows the Tenant to extend the lease for a further period (e.g. one year), at a pre-determined rent.

Penalty Clause: a clause in a contract which imposes a financial penalty when specified events occur or fail to occur (e.g. a failure to deliver on time). The clause may be unenforceable if the stated penalty is unreasonably high.

Personal data: are data relating to a living individual who can be identified from those data (see also "*sensitive personal data*").

Personal lease: a Lease or Tenancy Agreement where the Tenant is the individual Assignee (rather than the corporate employer).

Pro rata payment: a part payment of a fee for a service that is not fully completed.

Regulation: a form of EU legislation which passes into law automatically, in all EU countries, without any requirement for additional national legislation to be passed.

Restrictive covenant: a clause in an employment contract which restricts the ability of an employee to compete with an employer after the contract is terminated.

Sensitive personal data: this refers to personal 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")*

T&Cs: the terms and conditions contained in a contract.

Unfair dismissal: the termination of an employee's job unlawfully, due to the employer's failure to follow a fair procedure, or where the employer has acted unreasonably or has no valid reason for the termination.