WorkFlex

Data Protection

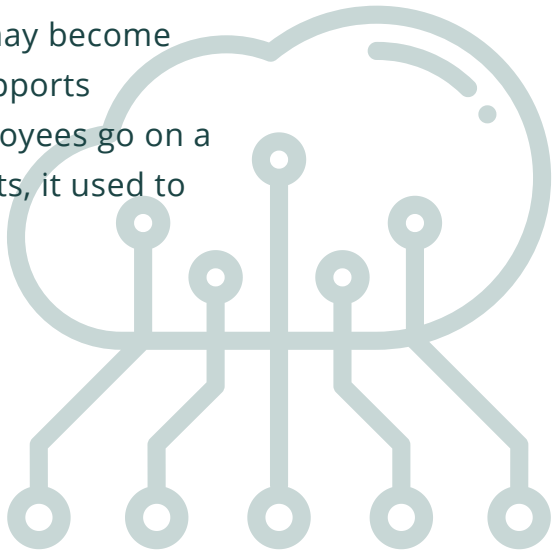
Ensuring compliance as employees work from abroad

Written by: Abdullah Magdi
Edited by: Pieter Manden
Research Assistant: Mostafa Alkadi

Table of Contents

PREFACE

When employees temporarily work from abroad, several compliance risks loom. The employee may constitute a so-called Permanent Establishment, a corporate tax topic. Another example is that local social security premiums may become payable in the destination country. WorkFlex supports employers with the compliance when their employees go on a workation or business trip. In its risk assessments, it used to analyse the following 6 risk dimensions:



- Permanent Establishment;
- Wage Tax;
- Social Security;
- Labour Law;
- Work Entitlement;
- Posted Workers Directive

Recently, a 7th risk dimension was added: data protection. WorkFlex is the only provider that considers data protection in its risk assessments, but this doesn´t mean that it is not important. On the contrary. This white paper describes how data protection is relevant when employees temporarily work from abroad.
In this paper, WorkFlex is going to tackle its comprehensive exploration of data protection and data security in the context of employees working from abroad in order to serve as a vital guide for organizations navigating the intricacies of safeguarding sensitive information. It is also crucial to emphasize that data protection and data security are distinct yet interrelated concepts, each with its key components and considerations.

The elucidation of key components of data protection, encompassing confidentiality, integrity, availability, consent and notice, purpose limitation, data minimization, security measures, data subject rights, and accountability, are going to provide a solid foundation for understanding the multifaceted nature of preserving the privacy and integrity of personal data.
Similarly, the exploration of key components of data security, including access control, encryption, firewalls, intrusion detection and prevention systems, security policies and procedures, data backups, physical security, security software, employee training, patch management, and security audits, will underscore the critical measures necessary to fortify the digital perimeter against evolving cyber threats.

DO NOT MISTAKE DATA PROTECTION FOR DATA SECURITY!

Despite the fact that the two terms are often used interchangeably, data security and data protection are not the same thing. Data security primarily concerns safeguarding data from unauthorized access, disclosure, alteration, or destruction. Data protection is more comprehensive, as it extends to protecting data from unethical use and unlawful control. Moreover, data protection involves policies, procedures, and legal frameworks to regulate the collection, processing, storage, and sharing of data in compliance with privacy laws and regulations. On the other hand, data security only involves technical measures to ensure data safety such as encryption, firewalls, antivirus software, and other security measures that are considered part of data security efforts.

Data protection

Data protection refers to the measures that are put in place to safeguard and secure personal and sensitive information from any breach. A breach can be unauthorized access, disclosure, alteration, or destruction. In the digital age, data protection is critical. After all, personal information is constantly being collected and processed by various entities, including governments, businesses, and online services. Data protection helps protect individuals from privacy violations, identity theft, and other forms of misuse of their personal information.

Overall, data protection remains relevant when employees work from abroad, and organizations need to adapt their data protection practices and policies to address the unique challenges and risks associated with this scenario. Ensuring compliance with applicable data protection laws and maintaining data security is essential for protecting the privacy and rights of individuals, whether they are working in their home country or abroad. Examining the key components of data protection will also demonstrate why it is highly relevant when employees temporarily work from abroad.

Key components of data protection

	Confidentiality	Integrity	Availability
Definition	Confidentiality ensures that access to data is restricted to authorized individuals or systems.	Integrity ensures the accuracy and reliability of data throughout its lifecycle.	Availability ensures that data is accessible when needed by authorized users.
Measures	Encryption, access controls, and user authentication are employed to maintain the confidentiality of sensitive information.	Implementing data validation checks, version control, and data integrity verification mechanisms help maintain the integrity of information.	Redundancy, backup systems, and disaster recovery plans are key components of ensuring data availability.

	Accountability:	Purpose Limitation	Data Minimization
Definition	Organizations are responsible for ensuring compliance with data protection regulations and are accountable for their data processing activities.	Limiting the collection and processing of data to specific, legitimate purposes disclosed to the individuals.	Collecting only the minimum amount of data necessary for the intended purpose.
Measures	Conducting privacy impact assessments, appointing data protection officers, and maintaining documentation to demonstrate compliance.	Clearly defining and communicating the purposes for which data is being collected and processed.	Avoiding unnecessary collection of personal information and regularly reviewing data retention practices

Security Measures	Data Subject Rights	Consent and Notice	International Data Transfers
Physical Security Protecting physical access to data storage facilities and devices. **Technical Security** Implementing firewalls, encryption, antivirus software, and other technical measures to safeguard data. **Organizational Security** Establishing policies, procedures, and training to ensure that employees handle data securely.	**Access and Rectification:** Among other data rights, individuals must have the right to access their personal data and correct inaccuracies. **Erasure (Right to be Forgotten)** Individuals have the right to request the deletion of their personal data under certain circumstances.	**Consent** Obtaining explicit and informed consent from individuals before collecting and processing their personal data. **Notice** roviding clear and transparent information to individuals about how their data will be used and processed.	Complying with regulations governing the transfer of personal data across borders, such as implementing appropriate safeguards for international data transfers.

Key taking:

"Data security is an essential part of data protection!"

Data security

Data security is the practice of protecting digital information, both in storage and during transmission, from unauthorized access, disclosure, alteration, or destruction. It is a fundamental aspect of information technology and cybersecurity, and it encompasses a wide range of measures and best practices aimed at safeguarding data from various threats, including cyberattacks, data breaches, and data loss.

Key components of data security include:

Access Control	Encryption	Firewalls	Security Software:
This involves managing and controlling who has access to specific data. Access control mechanisms can include usernames and passwords, biometric authentication, role-based access control, and encryption.	Data encryption transforms information into a format that can only be read with the correct decryption key. This ensures that even if unauthorized parties gain access to the data, they cannot understand it without the encryption key.	Firewalls: Firewalls are network security devices that monitor, and filter incoming and outgoing network traffic based on an organization's previously established security policies. They help prevent unauthorized access to data.	Employing antivirus software, anti-malware tools, and other security software can help protect against various forms of cyber threats.

Intrusion Detection and Prevention Systems (IDPS)	Security Policies and Procedures	Data Backups	Physical Security
These systems are designed to identify and respond to potential threats and intrusions in real-time, helping to protect data from malicious activities.	Establishing and enforcing security policies and procedures within an organization helps ensure that employees, contractors, and other personnel follow security best practices.	Regularly backing up data ensures that even if data is compromised or lost, it can be restored from a safe and secure copy.	Data security also encompasses protecting physical access to data storage devices, data centers, and server rooms.

Employee Training	Patch Management	Security Audits and Monitoring
Ensuring that employees are aware of security best practices, such as recognizing phishing emails or not sharing passwords, is a critical component of data security.	Keeping software, operating systems, and applications up to date with the latest security patches is essential to prevent vulnerabilities that can be exploited by attackers.	Regularly assessing the security of an organization's data infrastructure and monitoring for potential threats or breaches is crucial

In summary, data security is more focused on preventing unauthorized access and ensuring the confidentiality, integrity, and availability of data. Data protection, on the other hand, encompasses a wider set of principles and practices, including legal and ethical considerations related to the responsible handling of personal information.

DATA BREACHES WHEN EMPLOYEES TEMPORARILY WORK FROM ABROAD

The evolution of the modern workplace has been fundamentally reshaped by the rise of remote work, a trend accelerated by technological advancements and the changing dynamics of the global workforce.

As remote work becomes more viral everyday, it brings both opportunities and challenges, especially in the area of data security. Addressing data protection for employees working abroad adds complexity to the cybersecurity landscape as the data breached could be amplified, with increased risks like unsecured Wi-Fi networks, device vulnerabilities, and the diverse legal frameworks.

Phishing attacks already constitute a threat when employees conduct their business from secured facilities on computers that belong to the organization, and it continues when employees temporarily work from abroad. However, the complexities of international data transfers, remains on the top of the most common data protection threats when employees work from abroad.

1. Unsecured Wi-Fi networks

The nature of remote work has released employees from traditional office environments, allowing them to work from virtually any location with internet connectivity. While this newfound flexibility enhances productivity, it also introduces a significant cybersecurity risk—unsecured Wi-Fi networks. Employees working from abroad often rely on public or unsecured Wi-Fi connections, inadvertently exposing sensitive corporate data to potential threats.

What are the risks?

1. Data controlling and interception:

- Unsecured Wi-Fi networks lack encryption, making it easier for hackers to intercept, delete, or modify data that is transmitted between devices, these attacks called **eavesdropping attacks**. This creates opportunities for unauthorized access to confidential information, including login credentials and sensitive business communications.

2. Man-in-the-middle attacks:

- A man-in-the-middle (MITM) attack is a cyber-attack in which a threat actor puts themselves in the middle of two parties, typically a user and an application, to intercept their communications and data exchanges and use them for malicious purposes like making unauthorized purchases or hacking.

Attackers can exploit unsecured networks to conduct man-in-the-middle attacks. By intercepting and altering communication between the employee and the organization's servers, adversaries can manipulate data or inject malicious content into the communication stream.

3. Network spoofing:

- Cybercriminals can set up rogue Wi-Fi networks with names similar to legitimate networks, tricking employees into connecting to these malicious hotspots. Once connected, attackers gain unauthorized access to devices and potentially compromise sensitive data.

4. Password sniffing:

- Unsecured networks expose passwords to potential sniffing attacks, where attackers capture and decipher login credentials. This puts sensitive accounts, including corporate email and cloud services, at significant risk.

Best practices to mitigate the risks of unsecured Wi-Fi networks

Of course, the best practice for overcoming such threats would be to avoid connecting to unsecured Wi-Fi networks, by using personal mobile hotspots or secure portable routers. However, who doesn't love free internet!
When employees temporarily work from abroad, the number one reason for their travel is leisure, therefore, organizations can't bet their data security on the temptation of working from a restaurant/café on the edge of the world that provides free Wi-Fi.

1. Use Virtual Private Networks (VPNs):
At WorkFlex, we encourage employees through the employees' instructions to connect to corporate resources via VPNs, which encrypt data transmissions and create a secure tunnel between the user and the organization's network. This mitigates the risk of data interception on unsecured Wi-Fi networks.

2. Implement multi-factor authentication (MFA):
We also advice our clients to enforce MFA for access to corporate systems. Even if login credentials are compromised on an unsecured network, the additional authentication layer adds a crucial barrier against unauthorized access.

3. Secure access points:
If possible, provide employees with secure Wi-Fi access points, such as those utilizing WPA3 encryption. This ensures a higher level of protection against network-based attacks. Of course that might endure extra expanses for corporates.

4. Device security measures:
Corporates must ensure that employees' devices have updated security software, including firewalls and antivirus programs. These measures contribute to overall protection against potential threats on unsecured networks whether it's home or abroad.

2. Phishing attacks

Employees working from abroad are particularly vulnerable to phishing attacks, as the absence of on-site security measures and increased reliance on various communication channels create favourable conditions for hackers. Understanding the nuances of phishing threats and implementing robust best practices are paramount to protect corporate data.
Employees working from abroad may use personal devices for work-related activities. These devices might lack the stringent security measures found in corporate environments, making them susceptible to phishing attacks designed to exploit device vulnerabilities.
Furthermore, hackers may tailor phishing campaigns to exploit geographic and cultural nuances, making their fraudulent communications more convincing. Employees working in diverse locations may be targeted with messages crafted to resonate with local contexts.

Best Practices to mitigate phishing risks:

The first thing would be conducting regular and targeted phishing awareness training for remote employees. Educate them on recognizing phishing indicators, such as suspicious email addresses, unexpected attachments, and requests for sensitive information.
Moreover, organizations shall implement advanced email security solutions that employ artificial intelligence and machine learning to detect and block phishing attempts. These solutions can analyze email patterns and content to identify potential threats.

Once again, enforcing multi-factor authentication (MFA) for all remote access to corporate systems might be one of the best practices to prevent these attacks. MFA adds an additional layer of security, making it more challenging for attackers to gain unauthorized access even if login credentials are compromised.

3. International data transfer

When employees temporarily work from abroad, they are most likely traveling with their laptops. Thus, when going abroad there may be different regulations regarding the processing of data that are different to those in the country of origin, and since the employee's laptop has data stored on it, there should be compliance to the employee should also comply with the data transfer regulations in his/her home country.

International data transfer could become one of the most complex issues when employees temporarily work from abroad in terms of legal compliance. Especially, after the General Data Protection Regulation (GDPR) came into force in 2018 in the European Union (EU). As per Articles 2-3 of the GDPR, the GDPR is applicable on EU territories, and is applicable to the flow of personal and sensitive data on such territories. Therefore, it doesn't only apply to EU citizens and residents inside the EU. However, it also is applicable to all companies that process the personal and sensitive data of EU citizens, regardless of whether a company is based in the EU. Thus, the compliance of a company to the GDPR can extend far beyond the geographical area of the EU.

Over the past few years, international data transfers, especially those to the United States, have been prominently featured in the media, notably following the European Court of Justice's annulment of the EU/US Safe Harbor framework. Despite concerns, organizations will find reassurance in the fact that, for the most part, the General Data Protection Regulation (GDPR) doesn't introduce significant changes to the previous rules governing cross-border personal data transfers, largely maintaining the framework established by the Directive. However, unlike the previous regime with limited sanctions for breaching transfer restrictions, non-compliance with GDPR's transfer requirements can now result in the imposition of substantial fines, reaching up to 20 million Euros or 4% of annual worldwide turnover for undertakings.

Furthermore, the GDPR outlines specific conditions in Article 44 that must be met for transfers of personal data to third countries outside the EU to be permissible. While transfers to countries, territories, or sectors deemed to have an adequate level of protection by the Commission don't require specific authorization (Article 45(1)), the existing adequacy decisions under the Directive will remain valid under GDPR until amended or repealed (Article 45(9)). So, for the time being transfers to any of the following countries are permitted: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, United Kingdom, United States of America

Notably, GDPR have recently introduced new mechanisms, such as approved codes of conduct and certification mechanisms, to justify international transfers (Article 46(2)(e) and (f)), and derogations similar to those in the Directive allow transfers based on explicit informed consent, contract performance, public interest, legal claims, vital interests, and other specified grounds. Compliance with GDPR's restrictions on transfers demanded by non-EU authorities is crucial, with recognition or enforceability contingent on international agreements such as mutual legal assistance treaties.

WHAT IS THE WORKFLEX APPROACH FOR DATA PROTECTION'S SUB-ASSESSMENT?

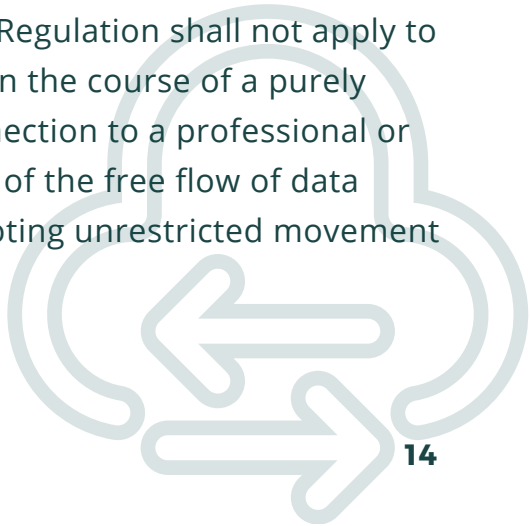
WorkFlex's message has always been to empower employees to work from anywhere, but with protecting employers from any compliance exposures. Recognizing the evolving challenges associated with a dispersed workforce, WorkFlex emphasizes flexibility without compromising security. We help organizations to navigate the compliance complexities of international data transfer.

In light of the aforementioned, WorkFlex developed a methodology for dealing with data transfers within and outside the European Union (EU) member countries. Of course, transferring data within the EU would be much less complex than transferring it to outside the EU due to the existence and enactment of the GDPR in these countries as well. Generally speaking, this means unified and adequate data protection standards, enforceable rights and remedies, in addition to the existence of European Data Protection Board (EDPB).1

What is the legal basis for free data transfer within the EU?

The legal basis for free data transfer within the European Union (EU) is established primarily through the General Data Protection Regulation (GDPR) and its associated principles. The key legal bases for free data transfer within the EU include:

1. Principle of free flow of data (Article 1(3) GDPR):
GDPR includes a specific provision, Article 1(3), "This Regulation shall not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity." which emphasizes the principle of the free flow of data within the EU. This principle is fundamental to promoting unrestricted movement of personal data across EU member states.2



2. Adequacy of data protection standards:
GDPR operates on the assumption that all EU member states adhere to a consistent and high standard of data protection. As it states in Article 45: "A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection." This principle of adequacy ensures that the legal frameworks and protections in place across the EU are equivalent, providing a solid foundation for the free transfer of personal data within the EU.

3. One-stop-shop mechanism
The GDPR introduces the "one-stop-shop" mechanism, allowing organizations to interact with a single lead supervisory authority (SA) based on their main establishment. This simplifies the regulatory process for organizations operating across multiple EU member states. The mechanism could be found in both articles 60 and 61 of GDPR:

- GDPR Article 60: "Each supervisory authority shall ensure that the tasks and powers assigned to it under this Regulation are carried out and exercised in accordance with this Chapter."
- GDPR Article 61: "Supervisory authorities shall cooperate with one another to the extent necessary for the performance of their tasks, in particular by exchanging information."

4. Intra-Group data transfers
While the primary focus is on avoiding reliance on derogations, Article 49(1)(a) of the GDPR allows for data transfers within a group of undertakings or enterprises for internal administrative purposes, provided the transfer is not repetitive and concerns only a limited number of data subjects.

5. Binding corporate rules (BCRs) (Article 47 GDPR):
GDPR Article 47 reads: "A group of undertakings, or one or more entities within a group of undertakings, may submit a draft of binding corporate rules to the competent supervisory authority, which shall provide an opinion on whether the draft rules (...) provide adequate safeguards throughout the Union."
This gives organizations the right to establish Binding Corporate Rules, which are internal codes of conduct for cross-border data transfers within a multinational group of companies. BCRs must be approved by the relevant data protection authorities and provide a legal basis for such transfers.

6. Standard contractual clauses (SCCs) (Article 46 GDPR):
The use of Standard Contractual Clauses, of which the European Commission approved by GDPR Article 46: "1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards." This is another legal mechanism for ensuring an adequate level of protection for personal data transferred between entities within the EU.

These legal bases collectively support the free transfer of personal data within the EU, allowing organizations to conduct business and collaborate across member states without encountering significant regulatory obstacles.

What organizations should consider before conducting an international data transfer outside the EU

It is already established that organization conduct international data transfer by allowing employees to temporarily work from abroad. When organizations conduct international data transfers outside the European Union (EU), they need to consider various factors to ensure compliance with data protection regulations and safeguard the privacy rights of individuals. We will go in depth of these factors as they are part of WorkFlex's approach to assess the legitimacy of international data transfer, but before that, a very important question forces itself; what would be the main objective here? What organizations should look for in a specific country before allowing data transfer?

Well, the European Commission developed something called an adequacy decision that simplify data transfers as they are considered secure with adequate safeguards for all privacy rights.

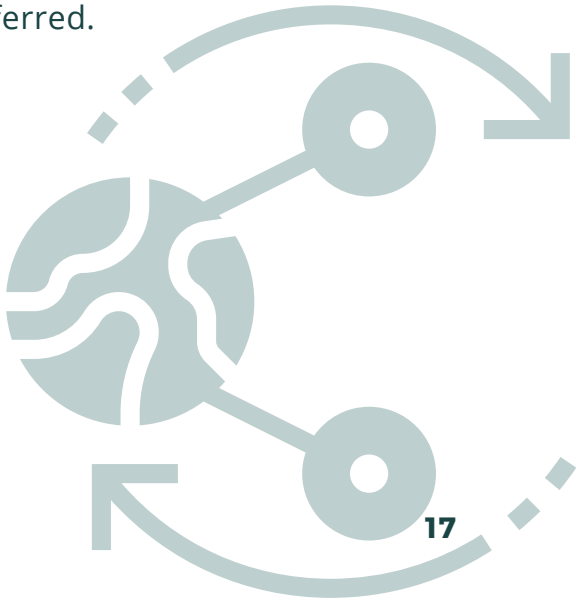
What is an adequacy decision?
An adequacy decision is an official determination made by the European Commission regarding the level of data protection provided by a third country or international organization. Specifically, an adequacy decision declares that the data protection standards and legal framework in the designated country or organization are deemed "adequate." This means that the level of protection for personal data in that country is considered essentially equivalent to the standards set out in the General Data Protection Regulation (GDPR) within the European Union (EU).

The criteria for granting an adequacy decision are outlined in Article 45 of the GDPR. These criteria include assessing the data protection standards, respect for individual rights, effectiveness of supervisory authorities, access by public authorities, judicial remedies, and other relevant factors.
The Commission don't require specific authorization (Article 45(1)), the existing adequacy decisions under the Directive will remain valid under GDPR until amended or repealed (Article 45(9)). So, for the time being transfers to any of the following countries are permitted: Andorra, Argentina, Canada (with some reservations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, United Kingdom, United States of America.

What if a country doesn’t have an adequacy decision?
In the frequently occurring case when an employee request a Workation from a country that is not within the EU nor has an adequacy decision, WorkFlex conducts a Transfer Impact Assessment (TIA).

What is Transfer impact assessment?
A Transfer Impact Assessment is a systematic evaluation conducted to assess the potential impact of transferring personal data from one location or jurisdiction to another. It involves a comprehensive analysis of the data protection and privacy implications associated with the transfer, ensuring compliance with relevant data protection laws and regulations. The purpose of a Transfer Impact Assessment is to identify and mitigate any risks or challenges that may arise during the transfer process.

When is a TIA required?
A TIA is prescribed by the GDPR when transferring personal data to a third country outside the EEA not covered by a European Commission adequacy decision. When people temporarily work from abroad, the fact that they have access to data from the other country already means data is being transferred.



What are the key components of WorkFlex TIA?

1. **General information of the data transfer.** This part contains general information such as the data importer and exporter, to which country the data will be transferred and the start and end date of the transfer.

2. **Sensitivity of the data being transferred.** This part categorises the data sensitivity level into 3 categories: a) Non-sensitive data: Publicly available or low-risk data, like contact details, person's name, job title, job history, educational qualifications, publicly available news or articles, publicly accessible business addresses, etc. b) Sensitive personal data: Information with potential harm or discrimination risks if mishandled, such as individual's address, passport number, social security number, financial or health records, racial or ethnic origin, religious beliefs, etc. c) Confidential and/or highly sensitive data: Legally protected, critical or regulated information with severe consequences if accessed or disclosed. For example, biometric data, genetic information, confidential legal documents, trade secrets, financial records, national security data, classified government information, etc.

3. **Country assessment:** In this part, WorkFlex assesses the adequacy of data protection in a specific country, through analysing and examining its data protection laws and regulation (in case of existence) along with GDPR alignment of these laws and regulations.

4. **Conclusion:** Where WorkFlex concludes a final overall result of the TIA, either Low Risk, Medium Risk or High Risk.

WORKFLEX ADEQUACY DECISION

WorkFlex has developed its own approach to assess country's data protection adequacy. We are adopting 11 factor criteria in order to assess the risk of Workation of individuals from abroad.

1. Is there a data privacy and security regulation in the jurisdiction?
The answer to this question is a Yes or No

2. How are the laws/regulations implemented?
The answer to this question is the level of hierarchy of the law, as in constitutional, a separate domestic legislation, articles in the civil/criminal code, etc... There could be several layers of law in this point, for example having a constitutional clause as well as domestic law.

3. Are there obligations to make notifications about personal data security breaches?
This factor will be answered firstly by a yes/no, then if the answer is a yes, there will be an examination of what specific cases will the data controller have to inform the data subject of a data breach.

For example this can be found in Article 19 of the GDPR where it states that "The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it."

4. Do data subjects have specific privacy rights that must be operationalized?
This factor will firstly be answered by a yes/no, then a further elaboration will be needed, as there are specific rights that should be guaranteed if the individual falls within the jurisdiction of the GDPR.

In the GDPR's Chapter 3 (Arts. 12-23) and Chapter 8 (Arts. 77-84) several rights are guaranteed for data subjects, most notably, their right to access their own data (Article 15), the right to rectification (Article 16), the right to erasure (Article 17), the right to restricting processing (Article 18), and the right to access an effective judicial remedy (Articles 78-79).

5. Are there restrictions on the transfer of personal data to third countries?

6. Transfers of personal data to third countries are permissible only if there is a legal basis for the processing/transfer?

Those two factors are intersecting, thus with regards to the first question it will be answered by a yes/no, then a further elaboration will be needed when it comes to the second question, as there are certain characteristics of transfers that should be complied with if there is an overlap with the GDPR's jurisdiction.

Chapter 5 of the GDPR (Arts. 44-50) lays out several factors to consider the transfer of data to third countries. One of which is the adequacy decision, where if the European Commission decides that the country or international organization that is going to receive this data has adequate safeguards (Art. 46) thus fulfilling the criteria laid down for data protection under the GDPR, then there will be no specific authorization decision required (Article 45 (1)), and in case of needing to transfer such data, then the commission can issue and adequacy decision (Article 45 (3). The criteria laid down for assessing such adequacy is outlined in Article 45 (2), where the 3 elements are:

a.) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

b.) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

c.) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

7. Are there accountability and governance requirements?

This is mainly a yes/no question, which stems from Chapter 8 (Arts. 77-84) where Arts. 78 and 79 govern the Right to an effective judicial remedy, Art. 82 outlines the Right to compensation and liability, Art. 83 outlines the general conditions for imposing administrative fines, and finally Art. 84 outlines the penalties that could be imposed by stating the following.

"Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive."

8. Are there separate laws or regulations regarding surveillance and/or technology which could be used for surveillance?

This is mainly a yes/no question, which stems from Arts. 6, 17, 18, 19, 21, 22, 23, and the aforementioned Art. 45 (2) (a). If there exists a law, the compliance of such law with the international standards would be the definitive factor as to what kind of risk this law would pose.

9. What is the risk of non-compliant data privacy and security practices for private sector organizations in the jurisdiction?

Non-compliance with data protection regulations may subject the data controller and/or processor to liability, compensation claims, sanctions such as fines (Arts. 82-84 GDPR). This is a specific example that is applicable for the data subjects that fall within the jurisdiction of the GDPR. Other jurisdictions may have different repercussions. Based on such repercussions, WorkFlex will be able to assess the level of risk posed by such penalties to our clients.

10. Is there an identified legal basis required in order to collect or process personal data or sensitive personal data in the employment context?

11. Is there an identified legal basis required in order to collect or process non-sensitive personal data?

Both questions trigger a yes/no question as a preliminary answer. In case the answer was no when it comes to the first question, then this would pose a data processing issue, as data processors and controllers generally need consent in addition to a legal basis to process personal and/or sensitive data. This legal basis can be in the employment context or for the public's interest for example. Please review Arts. 6, 7 and 9 of the GDPR.

Finally, based on the aforementioned 11 factors, there will be an adequacy decision issued. This adequacy decision will be based on the compiled result of the 11 factors, where the result will be either low, medium or high. This will be based on how the 11 factors rank, where each one could be green (Low), yellow (Medium), red (High) and consequently impacting the final adequacy decision of the data protection dimension.

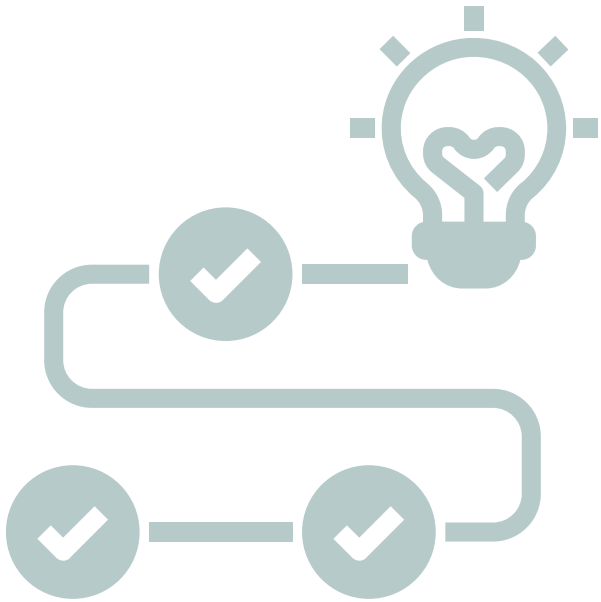
CONCLUSION

The landscape of remote work has ushered in a new era of flexibility and productivity, but it has also brought to the forefront the critical importance of robust data protection practices. As employees increasingly operate from abroad, organizations must navigate a complex terrain of potential data security threats.

The WorkFlex Approach for Data Protection's Sub-Assessment provides a strategic framework for evaluating the adequacy of data protection measures in specific jurisdictions. The examination of the legal basis for free data transfer within the EU, including principles such as free flow of data, adequacy of data protection standards, the one-stop-shop mechanism, intra-group data transfers, binding corporate rules, and standard contractual clauses, equips organizations with a roadmap for compliant international data transfers.

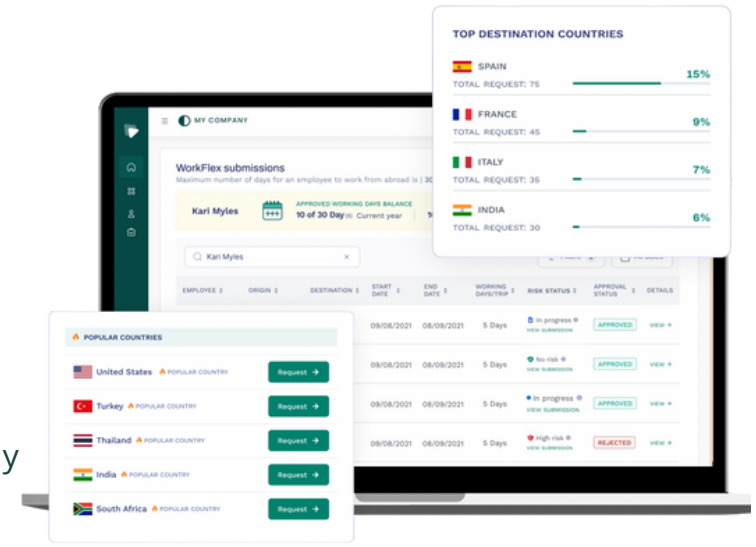
The analysis of what organizations should consider before conducting international data transfers outside the EU, coupled with insights into adequacy decisions and the WorkFlex Adequacy Decision framework, further empowers organizations to navigate the complex landscape of global data protection.

In conclusion, this whitepaper not only serves as a comprehensive resource but also as a call to action. As organizations continue to embrace remote work, the safeguarding of data must remain a top priority. By adopting the principles, best practices, and strategic assessments outlined in this guide, organizations can forge a path towards a secure, compliant, and resilient future, ensuring the protection of personal data in an increasingly interconnected and dynamic digital world, along with protecting employers from any potential compliance exposures, and that' why WorkFlex added a 7th risk dimension in its comprehensive risk assessment for temporarily work from abroad.

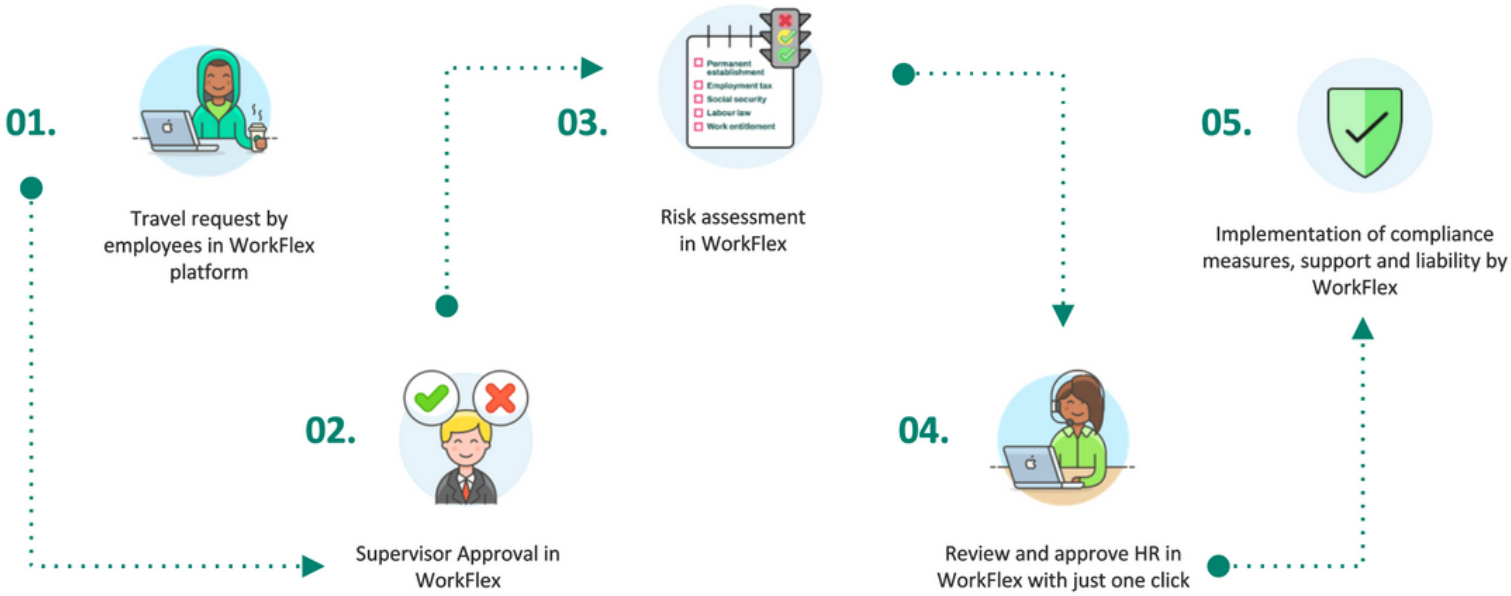


Our Solution

At Workflex we have developed intuitive software that allows employers to offer workations as an employee benefit - without any risks. With the help of our software, you can:



- **Eliminate compliance & insurance risks.** Workflex takes care of all compliance & tax risks workations may encounter. Corporate tax, payroll tax, social security, labor law and work authorization.
- **Reduce administrative costs.** No need to hire expensive lawyers or staff to handle workation requests. Avoid potential fines, interest, and penalties in the event that workation risks occur, as Workflex assumes liability.
- **Save time with 100% automated processes.** Manage workation requests on an automated platform and get assistance in handling documentation and possible negotiations with foreign authorities.



"At TIMOCOM, vacation and work are not opposites! Thanks to Workflex's smart and straightforward solution for compliance issues, administration combined with great customer support, our employees can work up to 120 days a year from abroad. Our TIMOs have already worked 2567 days abroad so far."

Luisa Schlüter
HR Business Partner at TIMOCOM

"We at allygatr love remote work! Whether it's a team workation or individual work from abroad - WorkFlex as a tool has reduced the administrative effort for us by more than 95%!"

Benjamin Visser
Founder & CEO of allygatr

Want to know more?

Do you want to offer mobile working as a benefit in your company and learn more about how you can enable this easily & efficiently with WorkFlex's all-in-one software? Our team is here to help you with advice & support!

+49 30 31197038

hello@getworkflex.com

Hundreds of employers trust WorkFlex