Remote Work – Employment and Data Protection aspects

Deloitte Legal Italy
29 settembre 2021
Welcome to breakout room – Employment and Data Protection Law

The speaker

Stefano Piero Luca Miniati  
Managing Associate  
Team Employment and Benefits  
+39 02 833 24053  
sminiati@deloitte.it

Francesca Gili  
Managing Associate  
Team Data Protection  
+39 02 833 24513  
fgili@deloitte.it
Contents

- Italian discipline of remote working
- Right to disconnection
- Law applicable to international remote working
- International public order
Italian discipline of remote working

What is smart working?

In Italy, remote work (or “smart working”) is regulated in Articles 18-23 of Law no. 81/2017.

Employer and worker sign an agreement by which they establish that the work is performed, also with forms of organization by phases, cycles and objectives:

- partly outside the company premises without a fixed location, within the limits only of the maximum duration of daily and weekly working time, arising from the law and collective bargaining;
- without precise constraints of time or place of work;
- with the possible use of technological tools for the performance of the work activity.

In the agreement, which must be in writing and may be for a fixed or indefinite period, the parties regulate the manner in which work may be carried out outside company premises.
In particular, it is necessary to regulate the following aspects:

- the employer's directive and control power is exercised;
- the worker's rest time;
- which are the tools used by the worker and the technical and organisational measures necessary to ensure the worker's disconnection from the them;
- the conducts that can be sanctioned at a disciplinary level.

In Italy the emergency legislation adopted to counter the spread of the Covid-19 introduced a simplified regime for “smart working”, to date valid until December 31, 2021. This simplified regime allows employers to activate “smart working” regime with a unilateral act, without an individual agreement, as instead provided for by Law No. 81 of 2017.
Italian discipline of remote working
Focus: Health and Safety

In this context, the employer is responsible for the safety and proper functioning of the technological tools assigned to the worker for the performance of the work activity.

In addition, the employer guarantees the health and safety of the worker who performs the service in modality 'of “smart working” delivering, at least annually, a written information in which are identified the general risks and specific risks related to the particular mode' of execution of the employment relationship.

The worker is obliged to cooperate in the implementation of the prevention measures prepared by the employer in order to face the risks connected to the execution of the service outside the company premises.

The worker has the right to protection against accidents at work and occupational diseases dependent on risks related to work performed outside the company premises.
International regulation

Under the international and UE regulation does not exist a legal framework regulating the matter, eve if the topic ir recently gaining more spaces in the main agenda of the relevant authorities.

In this respect on January 21, 2021, the European Parliament passed a resolution calling on the European Commission to submit a proposal for a directive to guarantee workers' right to disconnect (applicable to remote worker).

This requirement stems from the realization that the massive use of digital tools for remote work has led to the extension of working hours, blurring the boundaries between work and private life.

The main concept is that to refrain from working outside of working hours, without fear of sanctions or reprimands, should be considered as fundamental right of all workers.

! Today only a few EU Countries have recognized the importance of disconnection (among them France, Spain and Italy).
Law applicable to international remote working

INBOUND/ OUTBOUND remote working

When an employee works in two countries, a conflict of rules arises (between the rules of the country of origin and the rules of the country of destination). This conflict of rules is resolved by applying the criteria set out in domestic, European and international laws.

INBOUND:

- from EU countries → Regulation (EU) 593/2008;
- from non EU countries → Law no. 218 of May 31, 1995 (Italian private international law).

In this last case, a conflict of rules arises (between the norms of the country of origin and the Italian norms), which is resolved through the application of the selection criteria indicated in the Italian law of private international law.

OUTBOUND:

- to EU countries → art. 8 of Regulation (EU) 593/2008; local law regulating conflict of laws;
- to non EU countries → private international law; local law regulating conflict of laws.

In this last case, a conflict of rules arises (between the Italian norms and the norms of the country of destination), which is resolved through the application of the selection criteria indicated in the law of private international law of the country of destination.
Law applicable to international remote working

INBOUND

Today there is no specific discipline on international remote working.

Therefore, to identify the applicable law, the rules governing employment abroad apply. In particular, the relevant regulations are:

- art. 8 of Regulation (EU) 593/2008 if the employment relationship involves EU countries;
- art. 57 of Law no. 218 of May 31, 1995 if the employment relationship involves non EU countries.
Law applicable to international remote working

INBOUND - EU Countries

Art. 8 of Regulation (EU) 593/2008 states that the individual employment contract is governed by the law chosen by the employer and the employee or, in the absence of a choice, by the law:

- of the country in which the employee habitually performs the work, even if the employee performs it in another country on a temporary basis;
- if the above criterion is not sufficient, by the law of the country in which the employer's registered office where the employee has been hired is located;
- if even this last criterion is not sufficient, by the law of the country with which the contract appears to be more closely connected.

The choice of the parties shall not, however, deprives the employee of the protection granted by the provisions that is not possible to derogate by agreement under the law which, in the absence of choice, would have resulted as applicable under the criteria described above.
Law applicable to international remote working

INBOUND - Non UE Countries

Art. 57 of Law no. 218 of May 31, 1995 describes the way to identify the law applicable to contractual obligations with elements of internationality.

In particular, this regulation refers to the Rome Convention of June 19, 1980 on the law applicable to contractual obligations and it has been replaced by Regulation (EU) no. 593/2008 as of December 17, 2009.

The criteria that make possible to identify the law applicable to employment contracts with international elements are, then, now set out in art. 8 of Regulation (EU) no. 593/2008 (which, however, reproduces the same content as art. 6 of the Rome Convention of June 19, 1980 and, like this latter, identifies four criteria for identifying the law governing the employment contract).
Law applicable to international remote working

INBOUND - Non UE Countries

Art. 8 of Regulation (EU) 593/2008 states that the individual employment contract is governed by the law chosen by the employer and the employee or, in the absence of a choice, by the law:

- of the country in which the employee habitually performs the work, even if the employee performs it in another country on a temporary basis;
- if the above criterion is not sufficient, by the law of the country in which the employer's registered office where the employee has been hired is located;
- if even this last criterion is not sufficient, by the law of the country with which the contract appears to be more closely connected.

The choice of the parties shall not, however, deprives the employee of the protection granted by the provisions that is not possible to derogate by agreement under the law which, in the absence of choice, would have resulted as applicable under the criteria described above.
International public order

Applicable to EU and non EU cases

A limit to the application of foreign law is constituted by the so called “public order”, by which is meant the set of principles provided for the protection of fundamental rights of the individual, recognized at international level.

According to the most recent jurisprudential orientation, the notion of international public order includes the principles shared by the generality of state systems, excluding those principles that are peculiar only to a specific legal system.

At the present time, the main Italian rulesets that should be included in the principles of international public order are the following:

- minimum wage regulations;
- regulations on health and safety at work;
- rules governing the reasonable limitation of working time and vacation;
- rules governing termination (i.e.: notice period and protection against unfair dismissal);
- rules protecting maternity and prohibiting discrimination against women.

The above list, however, as anticipated, should not to be considered exhaustive, as the principles of public order, being the result of jurisprudential evolution, are general principles and changeable over time.
Law applicable to international remote working

OUTBOUND

To identify the applicable law, the rules governing employment abroad apply.

In particular, the relevant regulations are:

- art. 8 of Regulation (EU) 593/2008 if the employment relationship involves EU countries;
- private international law of the country of destination, if the employment relationship involves non EU countries.
Remote work deserves attention, particularly with regard to some fundamental aspects relating to the protection of personal data.
Remote work | Security Measures

Providing specific training sessions focusing on how to recognise and deal with social engineering attempts

Installing and configuring anti-virus and anti-malware software, ensuring that it is constantly updated

• Check for regular updates of the Operating System and other main applications used by the user
• Keep the firewall functionality of the individual device OS active

Allow remote access to company systems only through encrypted VPN tunnels to protect confidentiality and integrity of information

Provide encryption either of the hard disk of portable devices or of single volumes, folders or files containing personal data.

Implement solutions to remotely erase data stored on devices, e.g. in the event of loss/theft of a laptop

Back up information stored on devices in accordance with company guidelines (e.g., back up to a centralised system or local backups to removable media) and verify their validity and completeness

Ensure that smart workers access domain resources with minimal privilege user profile
Remote work | Policies and awareness

Internal policies should be defined and implemented within to provide clear rules for workers to follow:

- Defining guidelines for information management
- Defining or update the cyber security policy. Providing for specific roles and operations to be performed at the workstation affected by a security incident, through the adoption of an incident response policy
- Updating of the regulation for the use of IT tools
- Drafting a specific mobile device management procedure, identifying roles and responsibilities in relation to the operations to be carried out in the different phases of the mobile device life cycle.
- When the use of personal mobile devices for work purposes is allowed, the integration requirements should be clarified through a BYOD procedure.

Training for your employees

Human error is one of the main cause of...
Remote work

- International data flows
Under GDPR, data transfer abroad is subject to special precautions and rules.

### European Economic Area
(UE + Norway, Liechtenstein, Iceland)

The transfer of personal data within the European Economic Area is always allowed.

### Non EEA Countries

The transfer of personal data outside the European Economic Area to third countries is forbidden, unless the precautions specifically set forth by GDPR are taken (Articles 45-50).

---

Remote work | International data flows: principles set forth by GDPR
Remote work | International data flows: data protection guarantees

The GDPR confirmed the approach envisaged by Directive 95/46 regarding cross border data flows, providing for such flows they are forbidden, in principle, unless specific guarantees (specifically listed by the GDPR) are met:

- **Transfers on the basis of an adequacy decision (art. 45 GDPR)**
  A transfer of personal data to a non-EEA country may take place where the Commission has decided that such country ensures an adequate level of protection.

- **Transfers subject to appropriate safeguards (art. 46 GDPR)**
  In the absence of the adequacy decision a transfer of personal data to a non-EEA country may take place only if the Controller or Processor has provided appropriate safeguards (e.g., *standard data protection clauses, binding corporate rules,* ...).

- **Exceptions (art. 49 GDPR)**
  In the absence of an adequacy decision or of appropriate safeguards, a transfer of personal data to a non-EEA country shall take place only where one of the exceptions set out by Article 49 GDPR is met (e.g. data subject consent, relevant public interest ...).
The Schrems case

July 16, 2020 the European Court of Justice has invalidated the Privacy Shield, the framework for cross-border exchanges of the personal data of Europeans from the EU to the US. The judgment known as "Schrems II" has its roots in 2013, when Maximillian Schrems filed a complaint with the Irish Data Protection Authority, claiming that transfers of personal data under the EU-US Safe Harbor Agreement did not provide sufficient protection against access to data by public authorities.

PRIVACY SHIELD

The European Court of Justice has found that the surveillance programs of the United States interfere with the fundamental rights of persons, not limiting themselves to what is strictly necessary and proportionate, as required by EU law, and, therefore, do not meet the requirements of Article 52 of the Charter of Fundamental Rights of the European Union.

In addition, the Court has ruled that in relation to the US surveillance programs, EU stakeholders do not have a judicial remedy available to them and, therefore, are not entitled to an effective remedy in the US, as provided for in Article 47 of the EU Charter.

STANDARD CONTRACTUAL CLAUSE

The European Court of Justice has reaffirmed the validity of the standard contractual clauses but has stated that organizations must verify, on a case-by-case basis, whether the law of the recipient country ensures a level of protection for personal data equivalent to that required by GDPR; therefore, where the level of protection is not equal to that guaranteed in the European Union, the signing of the standard contractual clauses cannot be considered a suitable guarantee to allow a secure transfer of personal data subject to processing and organizations must provide additional measures or suspend transfers.
Remote work | International data flows assessment

Roadmap for the management of non-EEA data transfers: actions to do

Companies are called not only to be aware of every transfer put in place, but also to assess the risks to the rights and freedoms of the data subjects involved in such transfer and, subsequently, to choose the most protective tool and implement it effectively.

1. Identify the non-EEA transfers of personal data processed and update the Record of processing activities, if necessary.

2. Carry out a risk assessment in order to identify the risks connected to the data transfer and the most appropriate safeguards and security measures.

3. Assess if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards.

4. Identify and adopt supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence.

5. Take any formal procedural steps the adoption of your supplementary measure may require and re-evaluate at appropriate intervals the level of protection afforded.
Remote work | International data flows: an example

**EXAMPLE:** A US NATIONAL CFO, WORKING FOR AN ITALIAN COMPANY, CAN RETURN TO WORK TEMPORARILY FROM THE US BECAUSE OF THE PANDEMIC, WHILE CONTINUING TO MANAGE PERSONAL DATA (INCLUDING FINANCIAL DATA) CONCERNING THE ITALIAN COMPANY’S EMPLOYEES.

- does the simple fact that the CFO has access to the Italian company’s data constitute a cross-border data flow? how is this flow regulated?
Remote work | International data flows: an example

Transfer Impact Assessment (TIA) to be carried out before transferring personal data to the headquarter/subsidiary located in the US:

- Draft of a internal extra-EEA data transfer policy
- Preliminary assessment on data importer (TIA)
- Choice of the appropriate transfer tool, evaluating additional safeguards, if necessary
- Training addressed to employees on the matter

Answers to the Case study

Yes, the fact that the CFO has access to the Italian company’s personal data from the US is considered a cross-border data flow!!

Transfer Impact Assessment (TIA) to be carried out before transferring personal data from the EU to extra EU Countries even in the context of intragroup business activities.
Thank you for your attention

Avv. Stefano Piero Luca Miniati

Avv. Francesca Gili
Important notice

This document has been prepared by Deloitte Legal Società tra Avvocati a Responsabilità Limitata a socio unico for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of Deloitte Legal Società tra Avvocati a Responsabilità Limitata a socio unico to supply the proposed services.

The information contained in this document has been compiled by Deloitte Legal Società tra Avvocati a Responsabilità Limitata a socio unico and may include material obtained from various sources which have not been verified or audited. This document also contains material proprietary to Deloitte Legal Società tra Avvocati a Responsabilità Limitata a socio unico. Except in the general context of evaluating the capabilities of Deloitte Legal Società tra Avvocati a Responsabilità Limitata a socio unico, no reliance may be placed for any purposes whatsoever on the contents of this document. No representation or warranty, express or implied, is given and no responsibility or liability is or will be accepted by or on behalf of Deloitte Legal Società tra Avvocati a Responsabilità Limitata a socio unico or by any of its partners, members, employees, agents or any other person as to the accuracy, completeness or correctness of the information contained in this document.

Other than stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or insurance saving, no such conditions of confidentiality applies to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment.

Deloitte Legal Società tra Avvocati a Responsabilità Limitata a socio unico, a company, registered in Italy with registered number 2557295 and its registered office at Via Tortona no. 25, 20144, Milan, Italy, is an affiliate of Deloitte Central Mediterranean S.r.l., a company limited by guarantee registered in Italy with registered number 10788500964 and its registered office at Via Tortona no. 25, 20144, Milan, Italy.

Deloitte Central Mediterranean S.r.l. is the affiliate for the territories of Italy, Greece and Malta of Deloitte NSE LLP, a UK limited liability partnership and a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL, Deloitte NSE LLP and Deloitte Central Mediterranean S.r.l. do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2020 Deloitte Central Mediterranean. All rights reserved.