DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

To

Italian Data Protection Authority

Piazza Venezia n. 11, 00186 - Rome

Transmitted by PEC to protocollo@gpdp.it

SUBJECT: Contribution to the consultation on the retention period of metadata automatically generated and collected by e-mail transmission and sorting protocols

1. Introduction

On 21 December 2023, the Italian Data Protection Authority ('**Garante'** or '**Authority**') adopted the Guidelines entitled 'Computer programs and services for the management of e-mail in the work context and the processing of metadata' ('**Guidelines**').

The purpose of this Guidelines is to promote awareness among employers, both public and private, of the personal data protection risks that may arise from the use of computer programs and services for e-mail management, which are used daily in all work contexts, drawing attention to certain aspects that, in the Authority's view, could be in breach of the legislation in force. These systems, in fact, can collect in a preventive and generalized manner metadata on the use of e-mail accounts by employees.

The Guidelines does not provide a definition of what '*metadata'* are, making a generic reference to data '*relating to the use of email accounts in use by employees (e.g. day, time, sender, recipient, subject and size of the email)*', suggesting that they are a tool for monitoring employees because of the type of information processed through them.

The Garante specifies first of all that e-mail messages, as well as the external data of communications and attached files, are assisted by guarantees of secrecy protected by Articles 2 and 15 of the Constitution, in order to ensure respect for the dignity of the individual and his confidentiality. This implies that, even in the work context, there is a '*legitimate expectation of confidentiality in relation to the messages that are the subject of correspondence*'.

On these grounds, the Garante emphasizes the need for the employer as data controller,

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

(i) verifies the existence of an '*appropriate lawful prerequisite*' before the processing of workers' personal data through such programs and services, respecting the conditions for the lawful use of technological tools in the work context; and

(ii) put in place all the requirements for the protection of personal data, providing data subjects '*in a correct and transparent manner with a clear representation of the overall processing carried out*', thus enabling them to be fully aware of the characteristics of the processing even before it begins.

The employer, the Garante recalls, must scrupulously comply with the rules on remote controls laid down by Article 4 of Law no. 300/1970 ('**Workers' Statute**'), ensuring that the time taken to store metadata is proportionate to the legitimate purposes pursued and avoiding that a generalized collection and storage of such data may lead to indirect remote control of work activities.

The Garante therefore clarifies that the collection and storage of metadata may not exceed 7 days, which may be extended by a further 48 hours in the presence of proven and documented needs justifying its extension (e.g. for purposes of IT security and protection of the integrity of assets). In the event that the generalized collection and more extensive storage of metadata is required, the guarantees provided for in Article 4(1) of the Workers' Statute must be activated, ensuring in any case compliance with the principle of limitation of storage, as set out in Article 5(1)(e) of EU Regulation 2016/679 ("**GDPR**").

Following the adoption of the Guidelines, the Garante launched a public consultation on the appropriateness of the retention period for metadata identified therein, in response to numerous requests for clarification received. The Authority therefore invited public and private employers, data protection experts and any other interested parties to participate in the public consultation, submitting their comments to the Authority within 30 days of the publication of the notice in the Official Journal.

2. Why DLA Piper participates in the public consultation on the Guidelines

DLA Piper[1] is an international law firm that assists companies - both domestic and multinational - by providing support both in litigation before any criminal, civil and/or administrative authority, and out of court, in relation to all areas of law and all issues pertaining to corporate realities including, to the extent of interest herein, those pertaining to

[1] The following professionals from DLA Piper collaborated on this paper: partners Giulio Coraggio, Giampiero Falasca and Raffaella Quintana, associates Emma Benini, Francesca Cannata, Giorgia Carneri, Cristina Criscuoli, Nicola Di Iorio, Alessandra Giorgi, Federico Lucariello, Antonio Orsini and Matteo Pace, and trainees Matteo Antonelli and Matteo Nicoli.

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

the protection of privacy, labour law and *compliance* aspects in general. In this position, the Firm believes that it can provide the Garante with a useful point of view to implement and refine, where necessary, the Guidelines, with a view to loyal cooperation between subjects who, despite having different roles and positions, are united by the same purpose of protecting all legal assets of constitutional importance involved in the matter.

3. *Executive summary*

This contribution illustrates how the term of preservation of the metadata of corporate e-mails cannot be different from that applicable to the e-mails themselves, of which they are a fundamental component in order not only to allow them to function properly but also to preserve their authenticity.

Notwithstanding the above, the solution put forward by the writer is that company e-mails and their metadata should be retained for at least 10 years, not only to comply with legal obligations relating to the retention of correspondence but also to concretely protect the company's rights to assert and defend its interests, which are guaranteed by the Constitution.

In fact, any suspicious conduct requiring the analysis of company e-mails and related metadata may be discovered up to several years later, and this risk is even greater in a business environment where many employees increasingly work remotely.

This retention period cannot be the result of negotiations with trade union representatives or the Labour Inspectorate, because these entities would never agree to validate a period that deviates so considerably from the period stipulated by the Garante.

Retaining company e-mails and their metadata for 10 years would in any case protect employees because the employer could only access this data in the limited cases envisaged by the Garante itself in its guidelines and with the precautions provided for therein.

In addition, employers should inform their employees in advance by means of a detailed information notice on the processing of personal data, as well as conducting a DPIA and LIA.

4. Legal framework

4.1 Labour legislation

When the Workers' Statute was published in the Official Gazette on 20 May 1970, the text of Article 4 (then headed '*Audiovisual Equipment*') stipulated that the employer was

DLA PIPER

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

prohibited from using audiovisual equipment and other equipment for the purpose of remote control of workers' activities.

After almost 50 years, in a totally different world characterised by the widespread use of technology, the rule in question has been rewritten by Article 23 of Legislative Decree 151/2015, taking into account - on the basis of Delegated Law No. 183/2014 - the technological evolution that has taken place over time and the need to reconcile the productive and organizational needs of the company with the protection of the worker's dignity and privacy.

The new wording of Article 4, while maintaining the prohibition of remote control of workers' activities, has simplified the statutory rule, providing:

- an extension of the prerequisites of legitimacy for the installation of instruments from which the possibility of control also derives. While the need to reach an agreement with the trade union representatives or, failing that, to obtain authorisation from the Territorial Labour Inspectorate remains firm, the rule now provides that the requirements permitting the use of the aforementioned instruments no longer include not only organizational and production requirements or work safety, but also the protection of company assets (new Article 4(1)); and
- the exclusion from the obligation to reach a trade union agreement (or obtain ministerial authorisation), in the case of the use of tools used by the worker to perform work (so-called 'work tools') and tools for recording access and attendance, e.g. badges (new Article 4(2)). For example, PCs, tablets and company mobile telephones, which the worker needs on a daily basis to perform his or her duties, can be considered working tools. In this regard, the Ministry of Labour, already in 2015, specified that when the work tool is modified to monitor the worker (e.g. by adding special tracking software), the same tool no longer falls under the exception of Art. 4, para. 2 of the Workers' Statute.

In this context, it was therefore necessary, in order to prevent covert monitoring of work activities by the employer, that the worker be made aware of the various forms of surveillance to which he might be subjected. It is no coincidence that Article 4(3) - a sort of *trait d'union* between the *labour* world and the privacy world - makes a full reference to the relevant provisions on the protection of personal data, which the employer must comply with in order to operate a legitimate control over the workers concerned.

The employer must therefore provide the employee with comprehensive prior information on how to use the technological tools and how to carry out possible checks.

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

4.2 Personal data processing legislation applicable to the context

The law on the processing of personal data lays down a number of obligations on employers to ensure the confidentiality and dignity of employees. These obligations must be interpreted in the light of the principle of '*empowerment*' (Art. 5 of the GDPR), according to which the employer is responsible for adequately protecting the data of its employees, processing them in compliance with the applicable legislation and being able to prove it.

With specific regard to the processing of metadata associated with employees' e-mails, the employer must at least carry out the following activities:

(i) as just mentioned, provide employees in advance with concise, transparent and intelligible information on the processing of personal data that comprehensively describes the possible uses of e-mail (including the relevant metadata), the purpose and legal basis of the processing, together with the further details required under Article 13 of the GDPR. The employer is also required to explicitly state whether, to what extent and in what manner checks may be carried out. As indicated in the Garante's guidelines for electronic mail and the Internet, it may be appropriate to adopt an internal specification drawn up clearly and without generic formulas, which should be adequately publicised and periodically updated;

(ii) consider whether to carry out a prior data protection impact assessment, pursuant to Articles 35 and 36 of the GDPR, in the event of processing of metadata relating to the use of electronic mail for, inter alia, the performance of work and to assert and defend one's rights in connection with any litigation;

(iii) identify in advance an appropriate legal basis for the processing of metadata, in relation to each of the purposes for which it is processed. If the processing is necessary to enable the employee to perform his or her services, the legal basis will be Article 4(2) of the Workers' Statute (in conjunction with Article 114 of the Italian Privacy Code), whereas if the metadata is necessary to ensure IT security, the protection of the employer's assets or, more generally, the relevant rights, the legal basis could be Article 6(1)(f) of the GDPR;

(iv) carry out in advance a so-called balancing test for processing based on legitimate interest, in order to assess and demonstrate the legitimacy of the interest pursued, the necessity and proportionality of the processing and the prevalence of the employer's interests over the employees' rights, fundamental freedoms and interests;

DLA PIPER

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

(v) map the processing of metadata (and, in particular, the purposes pursued and the retention periods applied) in the register of processing activities, where adopted; and

(vi) take appropriate technical and organizational security measures to protect metadata against the risk of destruction, loss, modification, unauthorised access and disclosure and, more generally, to protect the confidentiality and dignity of workers.

In the case of the processing of metadata, the obligation set out in point (vi) above is particularly relevant with regard to determining the levels of access to metadata by the employer.

4.3. *Ex post* reconstruction of business facts and right of defence: regulatory profiles

Reconstructing, even after a long time, events that occurred in the normal, day-to-day business operations is an irrepressible need, as well as a duty for companies.

The possibility - or rather the necessity - to proceed with such reconstructions, not only responds to the obvious and basic defensive needs of entities in any forum (judicial or otherwise) but finds its primary foundation in the principles governing the very functioning of commercial enterprises.

In this respect, indeed, since the enactment of the Italian Civil Code in 1942, it has been an obligation for them, inter alia, to '*keep in an orderly manner for each business the originals of letters, telegrams and invoices received, as well as copies of letters, telegrams and invoices sent*' for a period of ten years from the date of the last registration (arts. 2214 and 2220 of the Italian Civil Code).

In even broader terms, in tax matters, Article 22 of Presidential Decree No. 600/1973 provides that, in the event of an assessment, compulsory accounting records and company correspondence must be kept even beyond the ten-year term provided for in Article 2220 of the Italian Civil Code, until such time as the assessment has been settled.

Evidently, in the current context in which telegrams, paper correspondence and invoices themselves have been totally superseded by e-mail, pec and electronic invoices, one cannot seriously doubt that the obligation to retain them for the prescribed time - 10 years or more in the case of a tax assessment - automatically extends to digital documents.

The obligation to preserve business correspondence (evidently today mainly digital) is therefore a duty that the law itself places on companies, which are required, by express

DLA PIPER

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

legislative provision, to trace the facts that affect the life of the company. In other words, therefore, it is the legislator himself who not only allows, but, in fact, imposes the *a posteriori* reconstructability of business facts.

On closer inspection, moreover, the tracing - and, to be more precise, the traceability - of company facts is not only a requirement of the legal system, but of the companies themselves in the exercise of the right of defence that is constitutionally recognised as inviolable (Article 24 of the Constitution).

In this sense, nowadays, there is no criminal, civil or labour, administrative or tax proceeding in which the company does not have the need (interest) to reconstruct and document company events, having the possibility to produce digital documents and, especially, company e-mails.

It is no coincidence that the Italian Supreme Court has recently clarified that an e-mail message (so-called "e-mail") constitutes an electronic document that contains the computer representation of acts, facts or legally relevant data which, even if unsigned, falls within the scope of computer reproductions and mechanical representations referred to in Article 2712 of the Italian Civil Code and, therefore, forms full evidence of the facts and things represented if the person against whom it is produced does not disregard its conformity with the same facts or things[2] .

Specularly with regard to the authorities' investigations, the Court of Auditors has stated that '*the main investigative means available to the tax authorities for carrying out tax control activities (...) is (...) computerised access, which guarantees, on the one hand, the conformity of the data acquired with the original data and, on the other, their* non-modifiability'[3] .

In a similar vein, confirming the centrality of correspondence in assessment activities, in the '*Operational Manual on Countering Tax Evasion and Fraud*', the Guardia di Finanza devotes ample space to computer analyses aimed at the acquisition of digital documents[4] .

Even more so in criminal proceedings, computerised correspondence often constitutes central evidence for the entire proceedings.

---

[2] See Cass. Civ., Sec. VI, 14.5.2018 no. 11606.
[3] See Court of Auditors, Deliberation No. 8/2018/G of 24 May 2018.
[4] Cf. Guardia di Finanza 'Operational manual on countering tax evasion and fraud' approved by Circular 1/2018 of 4 December 2017.

DLA PIPER

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

It is therefore not surprising that, over the years, the proactive use of defensive investigations by companies to reconstruct - even preventively - corporate facts in order to intercept possible *malpractices* and take timely countermeasures in the face of, for example, the following has become increasingly pregnant:

i. checks related to whistleblowing reports;
ii. criminal proceedings against senior management or employees or the entity itself pursuant to Legislative Decree 231/2001;
iii. inspection procedures of independent administrative authorities**;**
iv. legal action taken against the entity; and
v. offence committed against the entity.

These activities, which are governed in detail by Articles 327 *bis* and 391 *bis* et seq. of the Code of Criminal Procedure, include *digital forensics* activities*, which* fall within the scope of Article 391 *sexies of the* Code of Criminal Procedure, which allows the defence lawyer access to places available to the party. These include computer locations, such as, among others, company e-mail boxes, the usefulness of which is inextricably linked to the fact that e-mail messages are complete with *metadata* - such as sender, addressee, date and time, subject of the message - that guarantee their probative capacity.

The need to carry out defensive investigations **may emerge even several years after the relevant e-mails have been sent**, because any activities detrimental to the interests of the company are in most cases carried out in such a way as to circumvent the company's possible alert and verification systems. This is all the more true in the current economic context in which many employees work remotely at least some days of the week and can therefore more easily engage in conduct that would normally have aroused suspicion. In fact, the writer has observed in recent years **a considerable increase in litigation connected with, among other things, the misappropriation of confidential information and trade secrets** that were discovered even years after the employee had left the company.

It follows that the **deletion of the metadata within the period specified in the Guidelines would in fact make it impossible for the company to carry out subsequent investigations**. Similarly, the retention of this data only if a concrete suspicion of unlawful conduct emerges within the time limit set forth in the Guidelines would not be feasible because **the suspicion may emerge even several years later**.

5. The concept of metadata and its use in the employment relationship

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

With the Guidelines, the Garante per la protezione dei dati personali (Garante for the protection of personal data) took a position on the storage of so-called metadata inherent to so-called corporate accounts, such as, for instance, the day, the time, the subject of the e-mails, the size of the communication, and the sender and addressee.

In particular, the Garante considered that such metadata should be deleted after a retention period of 7 days (extendable by a further 48 hours, in the presence of proven and documented needs). This provision was then deemed surmountable by the Garante through the activation of the procedures provided for in Article 4(1) of the Workers' Statute.

The Garante arrived at this consideration by considering that the collection and storage of metadata, if limited to the above-mentioned time span, may fall under Article 4(2) of the Workers' Statute, since it would be information necessary to '*ensure the functioning of the e-mail system infrastructure*'.

If, on the other hand, this activity of collecting and storing metadata were to extend beyond the reasonable period indicated in the Guidelines, it would change its purpose in the sense that it would be based on the need to ensure computer security and the protection of the integrity of assets, "*as it could entail an indirect remote control of the activity of workers*", with the consequent lawfulness under the condition of Article 4(1) of the Workers' Statute.

Therefore, it seems useful to dwell on the notion of metadata and "working tools", in order to assess whether the metadata relating to the company email fall within this notion and whether, consequently, their use should be brought within the scope of Art. 4, paragraph 2, of the Workers' Statute which, as indicated in paragraph 4.1 above, provides for an exemption from the obligation of agreement/authorisation referred to in paragraph 1, for equipment and instruments which, although capable of determining a potential remote control, are used and necessary for the performance of work.

In 2016, Circular No. 2 of the National Labour Inspectorate clarified that 'instruments of work' within the meaning of the Workers' Statute are '*those apparatuses, devices, apparatuses and contrivances that constitute the indispensable means for the worker to perform the work performance deduced in the contract, and that for that purpose have been placed in use and made available to him*'.

Subsequently, jurisprudence has repeatedly had occasion to reaffirm that the company e-mail constitutes an indispensable means for the performance of work duties. In particular, '*the p.c. and the e-mail box cannot but be regarded as work tools necessary for the*

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

performance of work duties; consequently, the administrative and trade union duties provided for in Article 4 must be deemed unnecessary'[5] .

Again, more recently, the same judge had occasion to state even more expressly that '*the procedural authorisation regime does not [apply] to the tools used by the employee to render the work performance, such as, evidently, the PRS software and the* company *email*'[6] .

Moreover, the Garante itself came to the above considerations, when, in order no. 303/2016, it stated that '*the e-mail service offered to employees (through the allocation of a personal account) and the other services of the corporate network can be considered "work tools" in the sense of the above-mentioned legislation (i.e. Article 4(2) of Law no. 300/1970)*'.

It follows that it cannot in any way be argued that the company e-mail box constitutes a work tool and, therefore, falls under the derogatory regulation of Article 4(2) of the Workers' Statute, which excludes any need for the agreement/authorisation referred to in paragraph 1 above.

Having said this, it is considered that **metadata and the corporate e-mails to which they refer cannot but have the same discipline and the same storage term.** Metadata, in fact, are not only information relating to the e-mail message, but also **an essential element for the proper functioning of e-mail for their indexing and consequently their use.**

The inseparability of metadata from the relevant e-mails is also stated by the Agenzia per l'Italia Digitale ('**AgID**') in its guidelines on the formation, management and storage of computerised documents.

Given that e-mail undoubtedly falls within the notion of computer document as set out in the AgID guidelines[7] , these guidelines identify a set of mandatory minimum metadata to be associated with computer documents - as well as with computerised administrative documents and computerised document aggregations - which include the '*registration data*', i.e. those that associate a document with a date and a number, and the '*subjects*', including the author and sender of computer documents. This metadata must be present at all times in order to ensure that documents are preserved in accordance with the law.

Furthermore, it is stated in the AgID guidelines that '[t]he *computer document must be uniquely and persistently identified' and that the computer document preservation system*

---

[5] Court of Rome, Sec. Lav., order of 24.03.2017.
[6] Court of Rome, Sec. Lav., order of 13.06.2018, no. 57668.
[7] This is demonstrated by the definition of 'computer document' in Art. 1 of the Digital Administration Code (Legislative Decree 82/2005), according to which a computer document is any '*electronic document that contains the computer representation of legally relevant acts, facts or data*'.

DLA PIPER

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

must ensure, 'from taking charge until eventual discarding, the preservation of the following digital objects stored in it, [...]: a) computerised documents and computerised administrative documents with the metadata associated with them [...]'.

The above demonstrates the inseparability of the e-mails from their metadata and, therefore, the need to preserve the metadata until the end of the retention period of the e-mails to which they refer. In other words, without the metadata, it is not possible to "*ensure the functioning of the infrastructure of the e-mail system*"[8] , which is indispensable for the employee to be able to perform his duties.

The deletion of their information:

1. for the reasons set out above, would prevent the employer from properly storing business correspondence and thus from complying with the legal precept in Article 2220(2) of the Italian Civil Code and the tax regulations;
2. would not allow the correct use of e-mail by the employee himself and would therefore paradoxically harm the very employee that the Guidelines is intended to protect;
3. would sterilise the evidentiary value of e-mails, exposing the employer to challenges as to their authenticity by both employees and third parties and precluding the employer from asserting its rights in respect of any misconduct; and
4. could undermine the IT security and integrity of the employer's information assets, greatly increasing the risks of intrusion and other security incidents. Indeed, metadata analysis can be extremely relevant in determining the possible cause of a *data breach*. In addition, modern *antispam* solutions need historical data to determine whether an e-mail should be blocked and/or archived among junk mail. The deletion of metadata could therefore compromise the ability of companies and public administrations to effectively prevent and react to security incidents.

The lack of metadata would also make it complex or completely impossible to reconstruct ex post the facts of corporate life, including the possible detection of wrongdoing by employees or third parties.

On the one hand, in fact, the Document under Consultation damages the position of entities, whose right of defence, in any forum, would be irreparably compromised, as their ability to draw on the type of documents (such as company e-mails) that today have an often decisive evidentiary value is precluded.

[8] See page 2 of the Guidelines.

DLA PIPER

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

Similarly, paradoxically, not being able to acquire the complete e-mail metadata from the corporate e-mail *client* would also hinder or in any case slow down the investigators' own investigative activities.

The foregoing considerations also show how the lack of metadata associated with electronic mail could irreparably undermine the ability of workers to perform their work, as well as IT security, the effective exercise of the right of defence of the employer, workers and third parties, and the exercise of activities for the prevention, detection and repression of unlawful conduct by the public security authorities. This could have significant negative effects on the good performance of the public administration and on the efficiency and productivity of Italian companies, also compromising their competitiveness vis-à-vis foreign competitors.

The processing of metadata and that of e-mails must necessarily be regulated uniformly, as a separate use of one or the other instrument is not conceivable in fact.

In addition to the above, it is considered that the metadata cannot in any case '*lead to indirect remote control of employees' activities*'. In fact, **it is not clear how the limited information mentioned by the Guidelines,** such as *'day, time, sender, recipient, subject and size of the email'* **could actually allow indirect control of employees**.

This information, in fact, is necessary for the employee himself to be able to carry out his work activity. Extracting it without the relevant e-mails would provide extremely limited information about the work activity and would certainly not allow work activity to be monitored.

On the other hand, an employee who wanted to engage in misconduct or unlawful conduct could easily indicate a generic e-mail subject, send e-mails to an external account of his or her own, and limit the size of the message to a size that would not allow suspicious conduct to be identified. Possible **access to the metadata of company e-mails by the employer and the analysis of their content would in any case take place when the conditions indicated by the Garante in its guidelines for the analysis of e-mails are met** and to the extent that the Garante itself allows such analysis for the purpose of identifying possible unlawful conduct. Therefore, once again, the same legal treatment applicable to e-mails should be extended to the relevant metadata.

It follows that the legal regime applicable to e-mail metadata should be the same as the one provided for by the Garante with regard to e-mails in the Garante's guidelines for e-mail and the Internet. In that case, rather than providing for such a short retention period for e-mail metadata in the case of their processing for the performance of the employment relationship,

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

one should, as indicated below, adopt the much longer retention period that takes into account the purposes of the processing and limit access to the metadata with respect to the individuals who need it with respect to the different purposes of the processing and to circumstances in which the need for access is obvious.

As a further point of relevance, should the Garante not agree with the above-mentioned reconstruction, there remains the circumstance that the Authority's position according to which the metadata of corporate e-mails must be deleted after a retention period of 7 days (extendable by a further 48 hours, in the presence of proven and documented needs) **would in fact make it impossible for companies to agree with trade union representatives or the Labour Inspectorate on a term that is in line with corporate needs.** In fact, as already illustrated and as will be reiterated below, the company needs for tracking and documentation, as also imposed by law, require a deadline of at least 10 years from the sending of the e-mail. The Guidelines would in practice prevent companies from retaining metadata for the duration necessary to pursue the relevant purposes indicated above, **because no trade union representative or inspectorate would be in a position to depart so markedly from the term indicated by the Garante**.

In addition, the trade union representatives would probably refer the matter to the Labour Inspectorate. This would lead to an excessive number of requests to the Labour Inspectorate, which, in any case, for the reasons set out above is unlikely to take a course of action in line with the retention periods necessary for companies to pursue the above-mentioned aims.

In this way, on closer inspection, there is a clear compression of the right of defence, which ends up being conditioned i) to entirely aleatory and eccentric factors (the smooth running of industrial relations) or ii) to particularly burdensome fulfilments (obtaining authorisation from the National Labour Inspectorate), which appear *ictu oculi* incompatible with its constitutionally recognised inviolability.

6. DLA Piper's proposal

6.1. Criteria for identifying an appropriate retention period for metadata

In the preceding paragraph, it was pointed out that e-mail metadata represent - like the e-mails to which they refer and from which they appear hardly separable - a necessary tool for the performance of work, for a much longer period than the 7-day period indicated in the Guidelines.

DLA PIPER

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

Furthermore, it has been shown that metadata in itself does not allow for any monitoring of employees and has other indispensable functions, and its absence could cause serious harm to employers, employees and third parties interacting with them, as well as to the community as a whole. Therefore, it is considered that metadata should not be deleted until the e-mails to which it relates are deleted.

Given the retention limitation principle enshrined in Article 5 of the GDPR, it is now necessary to identify the criteria in the light of which an appropriate retention period for e-mails (together with their metadata) can be determined. In the next section, we will then illustrate the proposed solution to mitigate the risks associated with the retention of metadata.

It is considered that the retention period for e-mails should be determined by the employer, in accordance with the principle of 'empowerment'. In doing so, the employer must in any case take into account the term of

a) the obligation to keep accounting records provided for in Articles 2214 and 2220 of the Italian Civil Code;
b) the need to balance the right to privacy of workers with other constitutionally guaranteed rights, including the right of defence; and
c) the length of the statute of limitations of rights as provided for in our legal system.

On this point, it has already been mentioned (see *supra* 4.3.) that Articles 2214 and 2220 of the Italian Civil Code require the entrepreneur to keep the accounting records for 10 years from the date of the last registration. including the '*originals of letters, telegrams and invoices received, as well as [the] copies of letters, telegrams and invoices sent*' in connection with each business. It was also pointed out that, in even broader terms, the tax legislation provides for a possible extension of the retention period even beyond the ten-year period set by the Italian Civil Code, to ensure the assessment of income tax.

The letter of the law has a very broad scope and in the current business context there is no doubt that it should include all correspondence that companies exchange by e-mail in relation to their business. A different solution, in fact, such as an upstream check to verify individual e-mail messages and select the relevant ones, would be far more invasive for the privacy of employees and would entail the serious risk of resulting in an inadmissible constant monitoring of their behaviour. In any case, even if the e-mails relevant for compliance were selected and stored in a different archiving system, the lack of metadata would de facto jeopardise the possibility for the authorities to carry out legal investigations and for companies to use the e-mails to defend their interests because **the extraction of**

DLA PIPER

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

the e-mails in an archiving system would prevent the preservation of the information that would enable their authenticity to be verified.

In these terms, the legal obligation to keep correspondence for at least 10 years must inevitably extend to the metadata of company e-mails, which are an essential component of said correspondence. The same retention period must also be understood to extend to the use of data to enable the company to assert and defend its interests, otherwise it would not be able to protect itself against challenges by the competent authorities and third parties or conduct to its own detriment. It would therefore be a contradiction in terms, which is difficult to understand, to impose a retention of metadata limited to 7 days.

On closer inspection, the proposed solution appears to correctly balance the right to confidentiality of workers - and more generally of any individual whose data are contained in the employer's e-mail accounts - with the freedom of economic initiative, enshrined in Art. 41 of the Constitution and with the right of defence of the employer and of third parties (including other workers), protected under Article 24, which, as repeatedly reaffirmed by the Italian Supreme Court itself, prevails over the right to confidentiality of personal data, even in the context of labour relations and in favour of the employer[9] .

Considering therefore the evidentiary value attributed to e-mails (see 4.3. *above*) and the undisputed relevance of this tool for the activity of any company or public administration, the term of 10 years appears more than adequate to ensure the effective exercise of the right of defence of employees, employers and third parties interacting with them by e-mail as well as the effective exercise, by the public security authorities, of the activities of prevention, detection and repression of unlawful conduct, perpetrated in favour of or to the detriment of the employer.

Lastly, the ten-year term of retention of metadata proposed here also appears to be in line with the rules of prescription, meaning the period of time within which a person may assert a right before it expires.

The Italian Civil Code (Art. 2934 et seq. of the Civil Code) ordinarily provides for a ten-year limitation period, but, as is well known, there are cases in which the law identifies a shorter

---

[9] Cf., Cass. Civ., Sec. I, order of 13 December 2021, no. 39531, in which the Italian Supreme Court states that "*the principle according to which the interest in the confidentiality of personal data must yield in the face of the protection of other legally relevant interests, and configured by the system as prevailing in the necessary balancing act, including the interest, where genuine and not surreptitious, in the exercise of the right of defence in court, is identifiable*". See also Cass. Civ., Sec. Lav., judgment of 12 November 2021, no. 33809, in which the Italian Supreme Court reaffirms the principle that the right of defence in court prevails over the right to confidentiality of personal data, if such data are necessary for the purposes, precisely, of judicial protection, albeit in the presence of certain conditions.

DLA PIPER

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

period, such as non-contractual liability for damage caused to third parties (so-called tort liability), in which the limitation period is five years (so-called short limitation period), starting from the day on which the event occurred.

With regard to the statute of limitations for workers' rights, on the other hand, a distinction should be made between the rules applicable to salary claims and those relating to other rights arising from the employment relationship.

For workers' pay claims, the statute of limitations is five years and runs from the termination of employment, as per the recent Italian Supreme Court ruling No. 26246 of 6 September 2022.

In relation, on the other hand, to other rights deriving from the employment relationship, such as, by way of example, the recognition of a superior qualification or compensation for damage caused by mobbing, having a contractual matrix, the ordinary ten-year limitation period applies (Article 2946 of the Civil Code), which starts to run from the time when those rights can be exercised.

The time limit proposed here also appears to be in line with the statute of limitations for the administrative offence committed by entities, which, pursuant to Article 22 of Legislative Decree No. 231/2001, accrues within five years from the date of the commission of the offence.

In these terms, it is considered that the retention period for metadata cannot be shorter than the ordinary ten-year limitation period.

6.2. The recommended solution to mitigate the risk of monitoring workers

As seen above, the deletion of metadata in the terms indicated by the Guidelines could generate serious damage or inconvenience for a wide range of subjects, including workers, also undermining their ability to perform their work. Similarly, the need to reach an agreement with the trade unions or with the Labour Inspectorate would not be feasible in practice, not only because of the excessive workload to which the Labour Inspectorate would be subjected, but also because the Inspectorate would never agree on the considerably longer retention period necessary for the proper pursuit of the purposes indicated above.

In the writer's opinion, the only solution to adequately protect all the rights and interests at stake is to preserve e-mails and their metadata for at least ten years after the sending of each e-mail, regulating and radically limiting:

1. those who can access metadata and
2. the circumstances in which metadata can be accessed

DLA PIPER

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

only to scenarios where there is a concrete need to review such data, thus applying exactly the same principles that apply to access to corporate e-mails according to the guidelines issued by the Garante.

To this end, employers should determine in advance - in the internal rules referred to by the Garante in the guidelines for e-mail and the Internet - and in detail under what limited circumstances the employer or its agents may access employees' e-mail metadata, whether such access is by making a special request to the e-mail service provider or by surreptitiously entering the e-mail account. The specification shall also indicate precisely the procedure to be followed to obtain access to the metadata, the functions involved, the need to obtain authorisation from those within the organisation whose role is to ensure compliance with the law and internal policies (e.g. 'Legal' or 'Policy'), and the need to obtain authorisation from the person in charge of the organisation, the 'Legal' function or the 'Compliance' function), any possible exceptions to the aforementioned need for authorisation and the cases in which they are applicable, the criteria to be followed in carrying out checks on the metadata - in particular to ensure compliance with the principles of purpose limitation and data minimisation (Article 5 of the GDPR) - and the retention period for the metadata (and related e-mails) envisaged by the organisation. Furthermore, the metadata must be protected with appropriate measures to avoid the risk of abusive or indiscriminate access.

The solution identified above should be documented in a detailed DPIA, so as to ensure an adequate analysis of all risks, also related to the particularities of the concrete case.

We hope that the Garante can agree with the arguments put forward in this document and the proposed solution. Should this not be the case, we would like to draw the Authority's attention to the current unavailability of computer programmes and services for e-mail management, which would enable employers to comply with the requirements of the Guidelines.

In fact, no organisation today would be able to comply with the Garante's indications, except by radically renouncing the use of e-mail and exposing the company to considerable risks. This would create a scenario in which, in order to avoid exposure to litigation, potential cyber attacks, or impediments to business operations, companies would have to be able to incur a possible breach of the law on the processing of personal data.

For this reason, it is considered that, should the Authority confirm the orientation set out in the Guidelines or extend to a limited extent the deadline for storing the metadata indicated therein, it would be appropriate to grant public and private employers an ample 'grace period', so as to give them adequate time to comply with the Garante's requirements.

In thanking the Authority for the opportunity of discussion, we extend our best regards.

DLA Piper
Associated Tax Law Firm

Via della Posta, 7
I - 20123 Milan
T +39 02 80 61 81
F +39 02 80 61 82 01

Via dei Due Macelli, 66
I - 00187 Rome
T +39 06 68 88 01
F +39 06 68 88 02 01

P. VAT and Fiscal Code 12315050158

DLA Piper Studio Legale Tributario Associato