VI. Personal data

Glossary

Basic Health Law

Law no. 95/2019, of 4 September

CNPD

National Data Protection Commission

Decree-Law no. 20/2020

Decree-Law no. 20/2020, of 1 May, that amends the exceptional and temporary measures regarding the pandemic of the disease COVID-19

E-Privacy Directive

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector

EDPB

European Data Protection Board

GDPR

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of those data, and repealing Directive 95/46/EC (General Data Protection Regulation)

HSW

Health and Safety at Work

Law on the Protection of Data and Privacy in Electronic Communications

Law no. 41/2004, of 18 August, transposing into national legislation the e-Privacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector)

Law no. 1-A/2020

Law no. 1-A/2020, of 19 March, that establishes temporary and exceptional measures as a response to the crisis caused by SARS-CoV-2 and the disease COVID-19

Law no. 58/2019

Law no. 58/2019, of 8 August, implementing in national legislation the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of those data)

LFHSW

Legal framework governing health and safety at work (approved by Law no. 102/2009, of 10 September)

VI. PERSONAL DATA

VI.A. Background

When it comes to personal data protection, a number of issues have arisen on this subject with regard to how measures may be taken to prevent and mitigate the virus in compliance with the provisions of the GDPR, since the hazardous nature of the pandemic and the speed with which it has developed require rapid measures and, in certain cases, the processing of personal data which, in a normal situation, would not be necessary. Options such as temperature taking to allow access to premises (particularly, employee access to the workplace but also in schools), the use of fever screening thermal cameras and the use of location data and contact monitoring to prevent and fight infection, are under discussion, amongst other personal data relevant issues.

On 16 March, the Chair of the EDPB made a statement on the protection of personal data in the current context.[1] According to Andrea Jelinek, the GDPR does not hinder measures taken in the fight against the virus which involve the processing of personal data, and even provides for the processing of data in situations such as the one we are currently going through, but it must still be complied with. It is imperative that any adopted or envisaged measures comply with data protection provisions and principles and that no excessive data is collected, both in the current and futures stages and no prejudice is caused to data subjects rights and guarantees.

In late April, the EPDB issued guidelines on the processing of health data for the purpose of scientific research in the context of the COVID-19 outbreak.[2]

VI.B. Processing of personal data in the employment context: lawfulness

IDENTIFICATION OF THE PROBLEM

Various issues have been raised with regard to the processing of employee personal data in the context of measures adopted to prevent and fight the COVID-19 pandemic in the workplace, in that some of the actions require the processing of health data, which is particularly sensitive and consequently subject to especially strict arrangements under GDPR. As from the first moment, queries arose in relation to practices such as the following:

- Issuing questionnaires to employees, visitors and relatives regarding their recent travel and presentation of symptoms;
- Making it compulsory for employees to notify the employer of the existence of any employees considered 'suspected' or 'confirmed cases' of infection by the virus;
- Disclosing information to all staff with regard to the existence of 'suspected cases' or infected individuals among the employees;
- Taking the temperature to employees and visitors, including doing so with the help of fever screening thermal cameras.

LEGAL FRAMEWORK AND POSSIBLE SOLUTIONS

The processing of health data (*e.g.*, for the purposes of assessing whether an identified or identifiable individual is infected or is a 'suspected case') may only be carried out if one of the exemptions exhaustively laid down by Article 9(2) GDPR applies, since Article 9(1) prohibits the processing of data concerning

[1] Available at https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en.

[2] Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, adopted on 21-04-2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf (version with minor corrections 30-04-2020).

health (and of other special categories of data), unless one of these is met. The derogations laid down by Article 9(2)(b and h) may be invoked, depending on the circumstances of each specific case, providing a legal basis for the processing of health data in the employment context.

In fact, under Article 9(2)(b), the processing of health data may take place where 'processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject'.

The obligation to ensure a healthy workplace falls to employers under the **LFHSW** (approved by Law no. 102/2009), which lays down that the employer must provide the employee with safe and healthy conditions in all aspects of their work. Therefore, the collection of health data with a view to taking measures for prevention and containment (*e.g.*, monitoring employees showing symptoms of infection), including in the context of the steps that are gradually being taken for deconfinement and return to the workplace, is supported by compliance with such legal obligation.

Although in a smaller number of cases, the processing of data in the employment context may also take place for the purposes laid down in Article 9(2)(h), *i.e.* 'for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services'. Under Article 29(2) of Law no. 58/2019, 'in those cases provided for by Article 9(2)(h) and (i) GDPR, processing of the data referred to in Article 9(1) must be carried out by a professional bound to secrecy or by another person subject to a duty of confidentiality, and adequate information security measures must be taken'.

We must, therefore, take into account that:

- Along with the EDPB, a number of supervisory authorities have made statements regarding the processing of personal data, in light of GDPR, in the context of the current pandemic. Analysing the comments made by a number of supervisory authorities such as those in Spain, Italy, United Kingdom, Ireland, France and Portugal, the conclusion is that the measures to be implemented must take account, in light of the principles of necessity and proportionality, of the specific features of each organisation (*e.g.*, type of activity, individuals with risk factors) and those measures must be selected which involve the least possible intrusion, avoiding wherever possible the collection of special categories of data;
- Measures must be necessary and proportionate and taken to ensure the observance of the principle of minimisation, and all data subjects must be informed, in compliance with the principle of transparency;
- General and systematic collection of personal data must be avoided, except where justified (*e.g.*, compulsory temperature measurement and notification of immediate superiors), and the instructions of the competent authorities must be closely followed;
- Measures taken must not exceed the limits laid down by the competent authorities;
- Wherever possible, data must remain confidential, and in principle, unless strictly necessary, employees who are infected or suspected cases must not be identified to all staff, or must be identified only to the number of employees strictly necessary

to assess the risk of infection or to put quarantine measures in place;
- There must be specific channels through which information can be circulated within the company, with access limited to staff bound by a duty of confidentiality and to the extent strictly necessary.

The CNPD issued Guidelines on the collection and processing of employee health and private life data in the context of COVID-19 pandemic.[3] In these, the Portuguese supervisory authority specifically indicates that employers themselves must, neither proceed to the processing of staff health data (including temperature measuring or recording), nor to directly, collect and record additional information on risk situations or staff behaviour (that might indicate virus infection) and states that the processing of this type of employee data should only be performed in the context of the employers OSH services.

In such context OSH health professionals may:

(i) Evaluate employee health condition;
(ii) Request relevant information to assess employee's ability to render work in terms consistent with SST rules;
(iii) Adopt adequate proceedings to safeguard staff and third parties' health, whenever detecting symptomatic employees or in other justified cases.

The type and frequency of health evaluation measures must be determined by the OSH medical professionals according to: (*i*) scientific criteria adopted in their own clinical decisions; and (*ii*) national health authority guidelines.

The CNPD considers that employers' action should be totally aligned with DGS and other health authority guidelines – on how employers can protect their employees and what measures they should take in the workplace to prevent further spread of the disease – and that employers should not call upon themselves measures that result in the processing employee health data without being supported on specific legal provisions or on competent authority orders.

The guidelines were followed by legal provisions that point out to an opposite direction, as Decree-Law no. 20/2020, that amended exceptional and temporary measures on the COVID-19 pandemic now admits that employers may take employee temperature.

Under paragraph 1 of the new provision (Article 13.º-C) "in the present context of COVID-19, and exclusively for reasons concerning health protection of the employee and third persons, employee body temperature may be taken for the purposes of allowing employees access and permanence at the workplace." Paragraph 2 of this same legal provision foresees that "temperature recording referring to individually identified persons is expressly prohibited unless same person has given explicit authorisation for such recording", and under paragraph 3 "if temperatures are above the normal body temperature, the person may be denied access to the workplace."

In summary: the employer may monitor employee temperature to allow access to the workplace but not temperature recording may take place without employee consent. One may question, nevertheless, how the employer should document the grounds for access denial since such grounds involve the information that the employee temperature taken, on such occasion, was above normal levels. We would note that requesting employee's consent to record temperatures – and our understanding of the expression except when explicit authorisation has been given for such recording

[3] CNPD Guidelines issued on 23 April on the Collection and Processing of Employee Health and Private Life Data in the context of the COVID-19 pandemic (available at https://www.cnpd.pt/home/orientacoes/Orientacoes_recolha_dados_saude_trabalhadores.pdf).

may be interpreted differently – does not seem to provide legitimate basis for such processing insofar as in view of the imbalance of power that typically occurs in the employment context, it is unlikely that an employee would be able to respond freely to such request for consent.

Without prejudice of the above case not falling into the scope of the two explicit restrictions to employee consent that are set forth in Article 28, paragraph 3 of Law no. 58/2019, it would seem to us, in view of comments above, that explicit consent should not qualify as a legitimate basis (or permissive derogation) for employers to keep a record of employee temperatures measured for entry at the workplace, given that it is unlikely that the employee will not feel pressure to consent, impairing GDPR valid consent requirements to be met and such consent to actually mean a "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[4] Accordingly, we are admitting that if the temperature taken is higher than normal and employee being denied access to the workplace, it is advisable to involve the STT.

Additionally, it would have been advisable that rules were provided on the admissible methods to perform temperature monitoring; *e.g.* does the provision allow employers to resort to fever screening thermal cameras?

VI.C. Public interest and vital interest

IDENTIFICATION OF THE PROBLEM

Besides the processing of personal data in the employment context, some processing of health data cannot be based on the consent of data subjects, either because it is not feasible, or because this is not the most appropriate lawful basis. In some circumstances, public interest and vital interest, present in the need to combat the COVID-19 pandemic, may be taken as lawful bases for data processing, besides the consent of data subjects.

LEGAL FRAMEWORK AND POSSIBLE SOLUTIONS

Public interest and vital interest are conditions which can generally provide a legal basis for the processing of personal data, in particular by public bodies (Article 23 of Law no. 58/2019), for the purposes, for example, of monitoring epidemics and spread prevention (*i.e.*, humanitarian purposes).

In the context of the current pandemic, regardless of the existence of any other legal bases for processing, the processing of personal data (*e.g.*, the processing by law enforcement officers of declarations or certificates for the purpose of travel to work) may be lawful on the grounds of public interest or vital interest, as laid down by Article 6(1)(d) and (e) GDPR, which provide, respectively, for (*i*) the lawfulness of processing 'necessary in order to protect the vital interests of the data subject or of another natural person'; and (*ii*) the lawfulness of processing 'necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'.

Where the processing of data relates to special categories of data[5], account must also be taken of the exemptions enshrined in Article 9(2) (c), (g) and (i) GDPR, which provide that the general prohibition on the processing of special categories of data shall not apply, respectively, where: (*i*) processing is necessary 'to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent'

[4] Article 4, 11), GDPR.

[5] Data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation' (Article 9(1) GDPR).

(our view is that the scope of application of this legal basis to the current context will be quite limited); (*ii*) processing is necessary 'for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject' ; and (*iii*) processing is necessary 'for reasons of public interest in the area of public health, such as ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy'.

As regards the obligation on the controller to act in accordance with the law of the Member State (in this case, Portugal), emphasis should be given to the provisions of Base 35(2) of the Basic Health Law, which states that: 'in particular, the competent bodies shall be responsible for studying, proposing, executing and monitoring the measures necessary to prevent the importation or exportation of those diseases governed by the International Health Regulations, combating the threat of expansion of transmissible diseases and promoting all health operations required for the defence of the health of the international community'. Thus, similarly to what happens, for example, in Spain, the competent administrative bodies may bring forward urgent measures to combat the threat of expansion of COVID-19 and protect public health, in order to safeguard essential public interests, and controllers must cooperate and comply with any measures prescribed by the Public Administration.

It should be noted that vital interest can only be invoked where the processing cannot be manifestly based on another legal basis (Preamble, para. 46, GDPR).

Any personal data processed on the said legal bases must be limited to the minimum necessary in relation to the purposes for which they are processed ('minimisation of data'), and even though there may be an emergency situation for the protection of essential public health and/or vital interests, the fundamental right to data protection must continue to be respected (Preamble, para. 54, GDPR).

Thus, controllers must identify any processing of personal data which they carry out or seek to carry out in the context of the COVID-19 pandemic, assess which legal bases make such processing lawful and observe any recommendations made and still to be made by the CNPD in this regard.

VI.D. CNPD: suspension of time limits

IDENTIFICATION OF THE PROBLEM

In the current context, and by virtue of being in an exceptional situation, attention must be paid to the arrangements for (*i*) current procedural time limits, (*ii*) limitation and expiry periods and (*iii*) periods for compliance with obligations under applicable legislation by controllers (in particular, data breaches and exercise of rights by data subjects).

LEGAL FRAMEWORK AND POSSIBLE SOLUTIONS

The time limits for procedural acts to be carried out within ongoing civil, criminal and administrative proceedings are currently suspended – by Article 7 of Law no. 1-A/2019 – until the withdrawal of the special arrangements currently in place. The suspension of the time limits for these acts also implies the suspension of current limitation and expiry periods, including as regards the statutory compulsory maximum periods. The suspension of time limits for procedural acts also requires

the suspension of the limitation periods for any infractions committed by controllers.[6]

On the other hand, such suspension of time limits does not remove the need to comply, within the set time limits, with the obligations of controllers under GDPR and other applicable legislation, including the need to notify any breaches of personal data and the responses to the exercise of rights by data subjects.

VI.E. Remote working, confidentiality and security measures

IDENTIFICATION OF THE PROBLEM

One pressing matter, arising from the current requirement to prioritise remote working, arises from the need to comply with technical and organisational security measures in the processing of personal data.

LEGAL FRAMEWORK AND POSSIBLE SOLUTIONS

The requirement for remote working, provided that it is consistent with the functions carried out by the employee, creates the need for the employer to adapt, providing conditions for the performance of functions using appropriate technological means. This need will imply not only the provision of means which enable remote working (preferably the employer's own technological means), but also the creation of additional security measures in relation to data protection. Internal privacy and data security policies will need to be strengthened, as will the structure for allowing remote working.

Strengthening of remote access systems must include, inter alia, implementation of those applications necessary to allow remote access (such as applications intended for the authentication of users, extension of password expiry periods, VPNs and firewalls) and the constant updating and monitoring of the security of such applications. The crisis caused by the COVID-19 pandemic has already led to an increase in cybercrime, and therefore controllers must be aware of illegal activities of this kind, and constantly alert their employees to the risks which arise and create an effective channel for information exchange with internal IT staff.

Wherever employees use their own means, which will occur frequently, it will be appropriate to introduce Bring Your Own Device policies, where these do not already exist.

In the above context, the CNPD issued brief guidelines aiming at guaranteeing compliance of employee personal data processing under teleworking with the provisions governing personal data processing and protection and also at minimizing the impact on privacy of employee monitoring in the teleworking context.[7]

The CNPD indicates that the use of IT tools (*e.g.*, *TimeDoctor*, *Hubstaff*, *Timing*, *ManicTime*, *TimeCamp*, *Toggl*, *Harvest*) that allow detailed employee IT equipment activity monitoring or systematic collection of information on the employee's activity and inactivity moments is seen as being excessive personal data processing and, therefore, in breach of the principle of data minimization[8] and therefore considered as being inadmissible.[9]

---

(6) By decision issued on 16-03-2020 – Decision no. 2020/170 – the CNPD clarified that the time limits for entities and individuals to respond to notifications from the CNPD are interrupted until the end of the exceptional period as declared by the competent authority and will start to be counted from the beginning on the working day immediately following such declaration.

(7) Guidelines issued by the CNPD on 17 April on remote surveillance of telework employee available at https://www.cnpd.pt/home/orientacoes/Orientacoes_controlo_a_distancia_em_regime_de_teletrabalho.pdf.

(8) *Vid.* Article 5(1)(c) of the GDPR. The data controller, which in this context is the employer must limit data collected and further processed to the personal data that are (strictly) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

(9) For an indication on the options considered in these Guidelines for the employer to exercise its power of monitoring employee activity *vd.* Chapter IV.D, "Remote monitoring of employees teleworking" above.

As far as keeping working time records in teleworking the CNPD considers that in cases of teleworking, employers may resort to specific technological solutions and reminds employers that, for such purpose tools must have been "designed in accordance with the principles of privacy by design and by default, not allowing the collection of any information other than the data strictly necessary to pursue the mandatory worktime record purpose."[10]

VI.F. Processing of location data

IDENTIFICATION OF THE PROBLEM

As a result of the need to comply with quarantine and maintain social distancing, as well as other benefits (*e.g.*, detecting clusters of illness), there have been discussions about the benefits of sharing data – preferably anonymised and aggregated – by telecommunications operators with the authorities, with a view to monitoring locations where 'gatherings' are taking place and the requirements of confinement or social distancing are not being met. In addition, several private projects and initiatives have arisen which aim to monitor the virus and assist in its control. Although these data, contrary to health data, are not considered special categories of data within the meaning and for the purposes of the provisions of Article 9 GDPR, their processing is nevertheless subject to the special conditions enshrined in the Law on the Protection of Data and Privacy in Electronic Communications, a special law in light of GDPR.

LEGAL FRAMEWORK AND POSSIBLE SOLUTIONS

In an interview on 19 March[11], the President of the Italian Supervisory Authority (*Garante*) expressed his concern and stated that the state of emergency and the consequent compression of individual freedoms cannot justify excessive measures, such as proposals for mass digital screening, which should not be adopted rashly. In this sense, the collection of location and other data which enable the tracking of habits and movements should be the subject of considered analysis; the least restrictive measure should always be adopted.

In Italy, Germany and Austria, telecommunications operators have already shared anonymised and aggregated location data with health authorities, to assist with the monitoring of compliance with quarantine periods and social distancing, enabling the authorities to identify gatherings and movements. As these are anonymised data, *i.e.* they do not allow the data subjects to be irreversibly identified, this will not fall within the scope of GDPR. Nevertheless, since there is an intention to process personal location data and data ancillary to these checks and analyses (e.g. checks on the movement of persons in quarantine), GDPR should be observed, along with the applicable special legislation.

In Portugal, under Article 7(1) of the Law on the Protection of Data and Privacy in Electronic Communications, 'where location data are processed, alongside traffic data, in relation to subscribers or users of public communications networks or publicly-accessible electronic communications services, processing of such data is permitted only where they are made anonymous'.

In simple terms, location data may be shared provided that they are anonymous; where there is the intention to process location data in such a way that the data subject is identified or identifiable, such processing requires prior consent.

In any event, even in the present context, it is important to reduce to a minimum the degree

---

[10] In a clear reference to the principles of "data protection by design" and "by default" set-forth in Article 25 of the GDPR. For an indication on some of the worktime recording options CNPD specifically mentioned in the Guidelines on options *vd.* Chapter IV.D, "Remote monitoring of employees teleworking" above.

[11] Available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9292565.

of intrusion represented by mass collection of this kind of data, which must be carried out proportionately and only where strictly necessary.

Knowing that these issues have been the object of extensive discussion – and will continue to be so –, and that all stakeholders are turning toward the use of data driven solutions as part of the response to the COVID-19 pandemic, the EPDB adopted Guidelines[12], on the use of location data to analyse COVID-19 dissemination and the overall effectiveness of confinement measures as well as on the use of contact tracing applications.

The EPDB considers that it is preferable to develop a common European approach in response to the current crisis, or at least put in place an interoperable framework and that the efficiency gained from the use of this type of technologies depends upon the coordination with the health authorities.

As far as the use of location data is concerned, the EPDB emphasises that when it comes to using such type of data, preference should always be given to the processing of anonymised data rather than personal data and recalls the need to guarantee actual anonymisation that does not allow (re)identification of the data subjects. As noted by the EPDB "[t]he concept of anonymisation is prone to being misunderstood and is often mistaken for pseudonymisation. While anonymisation allows using the data without any restriction, pseudonymised data are still in the scope of the GDPR", similarly noting that location data (originating from telecom operators and/or information society services) which are known to be notoriously difficult to anonymise. On a final note on this specific issue, the EPDB highly encourages transparency regarding the anonymisation methodology given the complexity of anonymisation processes.

As far as contact tracing applications are concerned, in general terms and without going into detail on the different models under discussion, there use serves the purpose of informing users in case of contacted with someone that is subsequently confirmed as being infected.

For the EPDB it is essential that the use of such applications must rely on a voluntary adoption by the users given the grave intrusion represented by processing that involves systematic and large scale monitoring of location and/or contacts between natural persons.

The EPDB mentions that, ideally, if these applications are to be used, their use should be part of a comprehensive public health strategy to fight the pandemic, including, inter alia, testing and subsequent manual contact tracing, analysing possible infection chains and limiting the occurrence of false positives and incorrect data.

The EPDB stresses the need to give careful consideration to the principle of data minimization and data protection by design and by default, reminding that the tracing applications:

(i) Do not require tracking the location of individual users and that proximity data may be used instead;
(ii) Can function without direct identification of individuals and that appropriate measures should be put in place to prevent re-identification;
(iii) Must avoid data extraction and privilege solutions where collected information reside on the terminal equipment of the user, additionally guaranteeing that the relevant information is collected only when absolutely necessary.

Whenever the contact tracing applications involve storage and/or access to information

[12] Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

already stored in the terminal, which are subject to Article 5(3) of the E-Privacy Directive (transposed by Article 5 of the Law on the Protection of Data and Privacy in Electronic Communications – *i.e.* when it involves access to information stored in the terminal which does not qualify as traffic data –, the provider should seek the consent of the user.[13]

Disproportionate data retention mandates should not occur, and storage limitation should consider the true needs and the medical relevance (this may include epidemiology-motivated considerations like the incubation period, etc.) and personal data should be kept only for the duration of the COVID-19 crisis. Afterwards, as a general rule, EPDB recommends that all personal data should be erased or anonymised.

The EDPB notes that the mere fact that the use of contact-tracing applications takes place on a voluntary basis does not mean that the processing of personal data will necessarily be based on consent, the most relevant legal basis for processing being – when public authorities provide a service based on a mandate assigned by and in line with requirements laid down by law – the necessity for the performance of a task in the public interest under Article 6(1) (e) of the GDPR. Meaning: the upload and use of the application should be voluntary, but the subsequent data processing may have a different legitimacy basis to the extent the State Member in question has passed legislation on the use of such applications.

The European Commission also adopted a recommendation on 08-04-2020, setting-up a process for developing a common (European Union) approach, referred to as a *common Toolbox*, to use digital (technology and data) to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data.[14]

The toolbox consists of a number of practical measures for making effective use of technologies and data, with special focus on the following two particular areas:

> "(1) A pan-European approach for the use of mobile applications, coordinated at Union level, for empowering citizens to take effective and more targeted social distancing measures, and for warning, preventing and contact tracing to help limit the propagation of the COVID-19 disease […] involv[ing] a methodology monitoring and sharing assessments of effectiveness of these applications, their interoperability and cross-border implications, and their respect for security, privacy and data protection; and
>
> (2) A common scheme for using anonymized and aggregated data on mobility of populations in order (i) to model and predict the evolution of the disease, (ii) to monitor the effectiveness of decision-making by Member States' authorities on measures such as social distancing and confinement, and (iii) to inform a coordinated strategy for exiting from the COVID-19 crisis."

Following said recommendation a first iteration of a common EU toolbox was developed urgently and collaboratively by the e-Health Network with the support of the European Commission, providing a practical guide for Member States and explaining the essential requirements for national apps, namely that they be: (i) voluntary;

---

(13) Consent should be sought regardless of whether information qualifies as personal data or not. The exceptions to this consent requirement are those foreseen in sub-paragraphs *a)* and *b)*, or paragraph 2 of Article 5 of the Law on the Protection of Data and Privacy in Electronic Communications.

(14) Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID- 19 crisis, in particular concerning mobile applications and the use of anonymised mobility data, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020H0518&from=PT.

(ii) approved by the national health authority; (iii) privacy-preserving - personal data is securely encrypted; and (iv) dismantled as soon as no longer needed.[15] This was immediately followed by the adoption of guidance by the European Commission on Apps supporting the fight against COVID-19 and their development, setting out features and requirements which such apps should meet to ensure compliance with EU privacy and personal data protection legislation, in particular GDPR.[16]

The abovementioned guidance addresses only voluntary apps supporting the fight against COVID 19 pandemic "downloaded, installed and used on a voluntary basis by individuals (…) with one or several of the following functionalities:

- provide accurate information to individuals about the COVID-19 pandemic;
- provide questionnaires for self-assessment and for guidance to individuals (symptom checker functionality) (...);
- alert persons who have been in proximity for a certain duration to an infected person, in order to provide information such as whether to self-quarantine and where to get tested (contact tracing and warning functionality);
- provide a communication forum between patients and doctors in situation of self-isolation or where further diagnosis and treatment advice is provided (increased use of telemedicine) (…)."

---

[15] Mobile applications to support contact tracing in the EU's fight against COVID-19 – Common EU Toolbox for Member States adopted by the eHealth Network – voluntary network (platform of Member States' competent authorities dealing with digital health) set up under Article 14 of Directive 2011/24/EU – on 15-04-2020 available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[16] Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection (2020/C 124 I/01) available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=PT.

AUTHORS

Francisca Robalo Cordeiro
Associate

Maria da Assunção da Cunha Reis
Associate

Marta Salgado Areias
Associate

Tiago Félix da Costa
Partner

Member
Lex Mundi
World Ready

MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS

Supporting clients, anywhere, anytime.

MORAIS LEITÃO, GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS

LISBOA
Rua Castilho, 165
1070-050 Lisboa
T +351 213 817 400
F +351 213 817 499
mlgtslisboa@mlgts.pt

PORTO
Avenida da Boavista, 3265 – 4.2
Edifício Oceanvs
4100-137 Porto
T +351 226 166 950 - 226 052 380
F +351 226 163 810 - 226 052 399
mlgtsporto@mlgts.pt

FUNCHAL
Av. Arriaga, n.º 73, 1.º, Sala 113
Edifício Marina Club
9000-060 Funchal
T +351 291 200 040
F +351 291 200 049
mlgtsmadeira@mlgts.pt

mlgts.pt

ALC ADVOGADOS

LUANDA
Masuika Office Plaza
Edifício MKO A, Piso 5, Escritório A/B
Talatona, Município de Belas
Luanda – Angola
T +244 926 877 476/8/9
T +244 926 877 481
geral@alcadvogados.com

alcadvogados.com

HRA ADVOGADOS

MAPUTO
Avenida Marginal, 141, Torres Rani
Torre de Escritórios, 8.º piso
Maputo – Moçambique
T +258 21 344000
F +258 21 344099
geral@hrlegalcircle.com

hrlegalcircle.com

MdME LAWYERS

MACAU
Avenida da Praia Grande, 409
China Law Building
21/F and 23/F A-B, Macau
T +853 2833 3332
F +853 2833 3331
mdme@mdme.com.mo

HONG KONG
Unit 2503 B
25F Golden Centre
188 Des Voeux Road
Central, Hong Kong
T +852 3619 1180
F +853 2833 3331
mdme@mdme.com.mo

Foreign Law Firm

mdme.com.mo