COVID-19 Special

EU Member State Data Protection Authorities Deal with COVID-19: An Overview

*Christina Etteldorf**

Keywords: tracking of location data; processing of (health) data by public authorities; processing of employees' (health) data by employers; data protection in home office; (unsolicited) government contact via electronic communication; notification of information about the infection of a person; DPAs; coronavirus; COVID-19; data protection; GDPR

I. Introduction

The coronavirus currently overshadows all areas of our everyday life, whether professional or private. Social life as well as economy and trade are severely affected by its implications. Efforts to reduce the risk of infection and thus to stop or at least slow down the spread of the virus are forcing us to search for new solutions to maintain social and economic structures. Meetings that used to be held in person are now held by videoconference. Whether as a precautionary measure or due to ordered quarantine, the workplace is moved to the home (office). Governments, health ministries and medical research institutes are looking for technical solutions to track the spread of the virus and thus contain it. However, this also raises questions about the compatibility of these measures with (European) data protection law.

Is data processing by providers of videoconferencing tools, most of which are located outside the EU, lawful and can the use of these tools therefore also be justified vis-à-vis employees and business partners? Can sufficient measures be taken in the home office to ensure data security? May location data of infected persons be used to create movement profiles? Against the background of these questions, fears were quickly expressed that the strict data protection law, especially at EU level, would be an obstacle to the protective measures taken or to be taken against the spread of the virus, in particular that health protection measures and privacy protection measures would not be compatible. So which of the two should stand back? Or is there a way to reconcile both?

This question has been addressed by the data protection authorities (DPAs) of the EU Member States, which have issued statements giving advice on how to deal with data protection in the light of the current situation.[1] Since not all individual cases can be answered in a generalized manner, the main aim was to remind practitioners of the continued validity of data protection implications on the one hand, and to give them a little more (legal) certainty on the other. In particular, the fear that the GDPR would render Europe unable to act in the fight against the coronavirus were meant to be allayed. Accordingly, Andrea Jelinek, Chair of the European Data Protection Board (EDPB), stressed in her statement on the processing of personal data in the context of the COVID-19 outbreak[2] already mid-March that 'Data protection rules (such as GDPR) do not hinder measures taken in the fight against the coronavirus pandemic. However [...], even in these exceptional times, the data controller must ensure the protection of the personal data of the data subjects'. Considerations, which must necessarily be taken into account, have

* Christina Etteldorf, research associate with the Institute of European Media Law (EMR). For correspondence: <c.etteldorf@emr-sb.de>. Please note that this is a pre-print version; an updated version of the report will be published in the upcoming issue (2020) 2(6) EDPL. Last update: 30 March 2020.

1 For an overview of announcement and over relevant sources regarding data protection in light of COVID-19 cf cf the websites of the Global Privacy Assembly (GPA) <https://globalprivacyassembly.org/covid19/>, GDPRhub <https://gdprhub.eu/index.php?title=Data_Protection_under_SARS-CoV-2>, and , and the Europäische Akademie für Informationsfreiheit und Datenschutz <https://www.eaid-berlin.de/ressourcen-und-hinweise-zum-datenschutz-in-der-corona-krise/> which provide up-to-date information.

2 EDPB, Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak (16 March 2020) <https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_de>.

also been made by nearly[3] all DPAs of the 27 EU Member States although some DPAs[4] limited themselves to publish the EDPB statement on their websites. The priorities that were highlighted as being particularly relevant in this context will be presented below.

II. Relevant Topics of DPA Statements

1. Tracking of Location Data

Tracking of location data, which can be used to trace the movement of people that are proven to be infected with the virus and to draw further conclusions about the spread of the virus, also in order to warn those potentially at risk, is one of the first technical solutions that various institutes and governments have considered in the fight against coronavirus.[5] Since in the digital age almost everyone owns a smartphone that they carry with them at all times, in such measures telecommunications providers are regularly obliged to store connection data of their customers and applications such as Google Maps do the rest, the technical requirements for such or similar procedures are regularly already in place. Whether and how the data may be used by whom and for what purpose, however, is primarily a question of data protection law.

In this context, the EDPB points out that the EU data protection law does not hinder implementation of such technical solutions in general. In particular, when it comes to the question of the legitimacy of tracking measures, a distinction must be made between the tracking of individuals using various means of location determination, such as apps or access to telecommunications data, or the bundled transmission of summarised location data, from which the effectiveness of eg lockdown measures across the population can be deduced. However, certain requirements and limitations must be observed. In particular, public authorities should first seek to process location data in an anonymous way (ie processing data aggregated in a way that individuals cannot be re-identified), which could enable generating reports on the concentration of mobile devices at a certain location ('cartography').[6] Only if the processing of anonymised data is not possible or meaningful, personal data can be processed, although then the rules of the ePrivacy Directive[7] or its national implementation must be observed. The ePrivacy Directive generally requires the consent of data subjects for such types of data processing. However, the EDPB points out the possibility for Member States under Article 15 to introduce legislative measures pursuing national security and public security. This emergency legislation is possible under the condition that it constitutes a necessary, appropriate and proportionate measure within a democratic society. If such measures are introduced, a Member State is obliged to put in place adequate safeguards, such as granting individuals the right to judicial remedy. However, the EDPB warns that in any case the least intrusive solutions should always be preferred. Invasive measures, such as the 'tracking' of individuals (ie processing of historical non-anonymised location data) could be considered proportional under exceptional circumstances and depending on the concrete modalities of the processing.[8]

The announcements of the national DPAs, if any statements are made at all about tracking, essentially correspond to the statement of the EDPB. Even the Italian DPA expressed its support for the principles issued by the EDPB, stressing that despite the serious effects of the crisis, which are certainly devastating in Italy, it is not the time for improvisation.[9]

---

3 Only the Portuguese authorities have not yet published a position on the data protection implications of the Corona crisis on their website.

4 Maltese DPA, Press release of 20 March 2020 <https://idpc.org.mt/en/Press/Pages/Processing-of-personal-data-.aspx>; Cyprus DPA, Press release of 20 March 2020 <http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/9FD25484B6D041C4C225853100423083?OpenDocument>.

5 In doing so, they were likely inspired by the example in South Korea where the government tracked confirmed infection cases by using location and communication data. Cf <http://www.molit.go.kr/USR/NEWS/m_71/dtl.jsp?id=95083710>.

6 EDPB (n 2).

7 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 (Directive on privacy and electronic communications) [2002] OJ L 201/37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L 337/11.

8 EDPB (n 2).

9 Italian DPA, 'Interview with Antonello Soro' <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9294705>.

In particular, the Authority reserved the right to review the measures which, according to media reports[10], are currently already being implemented by authorities in Lombardy in order to verify compliance with the curfew by means of telecommunications data.

In response to a request from the European Commission, the EDPS has also taken a position on this issue.[11] Although the EDPS also states that '[e]ffectively anonymised data fall outside the scope of data protection rules', it points out that nonetheless, information security obligations under Commission Decision 2017/464[12] still apply. Also in this regard, the EDPS highlights the importance of ensuring data security (in particular in case of involving third parties to process the respective information) and data retention.

One special case in the context of using location data fighting the spread of the coronavirus is the Czech Republic. Here, the government has passed a corresponding government resolution to ensure better protection of the population. According to this resolution, the Ministry of Health is authorized to track the movement of people who are proven to be infected with COVID-19 – with their consent and after appropriate information – and to demand appropriate data from the telecommunications operators for this purpose.[13] The Czech DPA warns in this context that, nevertheless, the principles of data protection must be observed.[14]

2. Processing of (Health) Data by Public Authorities

The processing of data by public authorities and other public bodies is usually subject to specific rules at national level. Article 6 (2) and (3) GDPR give Member States room for manoeuvre, especially regarding the processing of data to fulfil a legal obligation or to perform a task carried out in the public interest. According to Article 9 (4) GDPR Member States may also implement special provisions on the processing of health data.

Correspondingly, in connection with data processing by public authorities, especially health authorities, against the background of coronavirus, the statements of the national DPAs regularly refer to the specific national law, which provides for corresponding legal bases and protective mechanisms.[15] Some countries have even already enacted current emergency laws, which also contain rules on the handling of personal data during the crisis. However, it is not possible to go into details of national rules in the context of this overview contribution. It should therefore only be pointed out here that the Spanish DPA, for example, has dealt extensively with the legal basis of the GDPR and its limits. In particular, Article 6 (1) (e) and (d) as well as Article 9 (2) (b), (c), (g), (h) and (i) GDPR are mentioned as the legal basis for data processing in connection with the coronavirus.[16] In the context of data processing by health authorities, the Lithuanian DPA also specifically mentions Article 6 (1) (c), (d) and (e) as well as Article 9 (2) (c) (in exceptional cases only), (g) and (i) GDPR.[17] However, reference is made in particular to Recital 46, which contains provisions on data processing for reasons of vital interests of the data subjects. According to this, the processing of personal data should be regarded as lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person but should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring

10 Cf Reuters report <https://www.reuters.com/article/us-health-coronavirus-europe-telecoms/european-mobile-operators-share-data-for-coronavirus-fight-idUSKBN2152C2>.

11 EDPS comment concerning Monitoring spread of COVID-19 (25 March 2020) <https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf>.

12 Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission C/2016/8998 [2017] OJ L 6/40.

13 Resolution no 250 of 18 March 2020 <https://apps.odok.cz/attachment/-/down/IHOABMTJPDJA>.

14 Czech DPA, Press release of 20 March 2020 <https://bit.ly/2xEeTT2>.

15 Swedish DPA (n 21); Polish DPA (n 24); Czech DPA, Press release of 13 March 2020 <https://www.uoou.cz/uoou-ke-nbsp-zpracovani-osobnich-udaju-v-nbsp-souvislosti-s-nbsp-sirenim-koronaviru/d-40538>.

16 Report from the State Legal Service Department (the Spanish DPA) on processing activities relating to the obligation for controllers from private companies and public administrations to report on workers suffering from COVID-19 <https://www.aepd.es/es/documento/2020-0017-en.pdf> (English version).

17 Lithuanian DPA, Press release of 23 March 2020 <https://vdai.lrv.lt/lt/naujienos/asmens-duomenu-apsauga-ir-koronavirusas-covid-19-papildyta-kovo-23-d>.

epidemics. The Spanish DPA also stresses the increased importance of the purpose limitation principle regarding the processing of health data, as explicitly mentioned in Recital 54.[18]

It is interesting to note in this context that many of the national DPAs are also concerned with the question of when the data collected in relation to the coronavirus should be classified as health data and thus as special categories of personal data. The Greek DPA clarifies in its guidance that the information that a person has been exposed to a health risk (for example, because he or she has been in a risk area or his or her partner is infected) is considered not to be health data.[19] This is also the view of the Finnish[20] and the Swedish DPA. The Swedish DPA differentiates furthermore the information according to if someone is in quarantine (no health data) or if someone has been quarantined under the Infection Protection Act (health data).[21]

3. Processing of Employees' (Health) Data by Employers

Employers, in particular, currently have a heightened interest in being informed about the health status of their employees, especially in order to be able to take the necessary measures to protect the health of the entire company staff. In its statement, the EDPB is cautious about the processing of employee data by employers and refers significantly to the relevant national law that regulates special protection obligations of employers. Employers should only access and process health data if their own legal obligations require it.[22] This includes in particular national rules of occupational health and safety law or sectoral professional law, which cannot be dealt with in detail in this report. Consequently, many DPAs make substantial reference to the instructions of the health authorities, which have often already issued guidelines for employers.[23] In addition, in the light of the corona crisis, some countries have already enacted emergency legislation that separately regulates the conditions employers must observe. In Poland, for example, the tasks, especially instructions from authorities to employees, are bundled and assigned to the Chief Sanitary Inspector as the competent authority.[24] In Italy, too, special obligations are imposed towards the public health authorities by the emergency legislation.[25]

The notification of data protection implications by national DPAs therefore varies widely in approach and scope. Nevertheless, commonalities can be identified in the setting of priorities. Statements on possible measures taken by employers can be roughly divided into information gathering by the employers (such as requesting information or filling in questionnaires by employees) on one hand and actual measures (such as temperature measurements of employees) on the other.

a. Information Gathering by Employers

When asked about the limits of information gathering by the employer, the DPAs seem to make a gradual distinction, which can be identified by taking an overall look at the various statements. This classification can be based on the degree to which different measures interfere with the employees' privacy. The request for health records or files by the employer is particularly drastic. Somewhat less intensive is the request to fill out predefined questionnaires with information on the health status. Finally, the question arises as to when the employer can ask the employee which specific questions about his or her state of health, or whether it must remain a general request for cooperation to all employees.

With regard to the request for records and medical documents by the employer, the national DPAs seem to broadly agree that this is not compatible with

18 Spanish DPA (n 16).

19 Guidelines for the processing of personal data within the management of Covid-19 (18 March 2020) <https://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=163,39,44,101,194,223,3,99>.

20 Finnish DPA, Press release of 12 March 2020 <https://tietosuoja.fi/en/artikkeli/-/asset_publisher/tietosuoja-ja-koronaviruksen-leviamisen-hillitseminen>.

21 Swedish DPA, Press release of 13 March 2020 <https://www.datainspektionen.se/nyheter/coronavirus-och-personuppgifter/>.

22 EDPB (n 2).

23 Luxembourgish DPA, Press release of 10 March 2020 <https://cnpd.public.lu/en/actualites/national/2020/03/coronavirus.html>; Belgian DPA, Press release of 13 March <https://www.autoriteprotectiondonnees.be/covid-19-et-traitement-de-donn%C3%A9es-%C3%A0-caract%C3%A8re-personnel-sur-le-lieu-de-travail>, by highlighting that the measures of other (health) authorities are also compatible with data protection law if they respect the principle of proportionality.

24 Polish DPA, Press release of 11 March 2020 <https://uodo.gov.pl/en/553/1103>.

25 Cf on this: Italian DPA, Press release of 20 March 2020 <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9282117>.

principles of data protection law without specific regulation. For example, the Hungarian DPA strictly rejects the requirement of health documentation by the employer.[26] This view is shared by the Estonian DPA by pointing out that the request for medical documents would require a contractual or legal basis.[27] In some professions, for example, this is often already provided for in the employment contract (eg in medical professions) – a possibility which the Austrian DPA highlights, too.[28] Moreover, the Estonian DPA considers it unlikely that a general legal basis for the request of medical records by employers will be implemented by the legislator even in emergency situations. The authority therefore calls on employers and employees to voluntarily provide information on their state of health.[29]

On the other hand, the views of the national DPAs are somewhat more divergent as regards the employer's requirement that his employees fill in predefined questionnaires. The Luxembourgish DPA[30] strictly rejects this as well as the French DPA and the Belgian DPA[31]. This applies in particular to predefined questions on health data, which are subject to special protection under Article 9 GDPR. According to the French DPA, the special protection under Article 9 GDPR means that employers may not *systematically* collect health data, covering inter alia predefined questionnaires.[32] On the other hand, the Hungarian DPA deems it acceptable to have the employees complete questionnaires, if based on a preliminary risk assessment carried out by the employer in advance, the employer concludes that the application of this method is necessary and it proportionately restricts the right of employees to privacy. This may then be used to ask questions about the date of the report, the personal data of the employee for the establishment of their identity, the fact of whether or not the venue and date of the employee's foreign travel, even if for a private purpose, coincides with the territories (countries) and periods listed in the employer's information material, the data concerning the fact of having contact with a person arriving from the territories indicated in the employer's information material. Article 6 (1)(f) GDPR is mentioned as appropriate legal basis. However, the questionnaires may not include data concerning the medical history of the data subject in light of Article 9 GDPR.[33] The Austrian DPA seems to take a similar view, for example, by allowing employers to collect contact details of visitors in order to be able to contact them in the event of an infection in the company.[34] The Irish DPA, on the other hand, wants to make the legality of questionnaires dependent on the existence of certain heightened risk factors indicating their necessity, such as the fact that certain professional groups or positions are generally associated with higher levels of travel activity or that there are particularly vulnerable people in the workplace.[35] The Greek DPA also does not want to exclude the possibility of the completion of questionnaires on residence and health status, at least not per se. In doing so, the Greek DPA refers to the current critical times and the unforeseen circumstances they imply. However, such measures could only be taken with particular regard to the principles of proportionality, data minimisation and adequacy.[36]

Without explicitly mentioning whether this is also possible in the form of questionnaires, the German DPAs and the Estonian DPA are of the opinion that employers may request certain information from their employees. According to the Estonian DPA, it should be possible to ask employees whether they have been exposed to a risk of infection or have symptoms of illness. In addition to the national rules of occupational health and safety law, Article 6 para. 1 lit. a, b, c and e GDPR are considered possible legal bases. The balancing of interests according to Article 6 para. 1 lit. f should also be a possible basis, as long as it is a question of requesting information about risks and not symptoms (health data). However, the

26 Hungarian DPA, 'Information on processing data related to the coronavirus epidemic' <https://www.naih.hu/files/NAIH_2020_2586_EN.pdf> (English version).

27 Estonian DPA, Press release of 16 March 2020 <https://www.aki.ee/et/uudised/kas-tootajat-saab-kohustada-raakima-koike-oma-tervislikust-seisundist>.

28 Austrian DPA, 'FAQ on data protection and coronavirus' <https://www.dsb.gv.at/documents/22758/23115/FAQ_zum_Thema_Datenschutz_und_Coronavirus_Covid-19.pdf/7cff6131-aed3-4bf5-8515-b724c82915a9>.

29 Estonian DPA (n 27).

30 Luxembourg DPA (n 23).

31 Belgian DPA (n 23).

32 French DPA, Press release of 6 March 2020 <https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles>.

33 Hungarian DPA (n 26).

34 Austrian DPA (n 28).

35 Irish DPA, Press release of 6 March 2020 <https://www.dataprotection.ie/en/news-media/blogs/data-protection-and-covid-19>.

36 n 15.

authority appeals far more to 'common sense', which in the current crisis situation requires full cooperation between employees and employers. It is 'not the time to stubbornly assert rights'[37] – a pathos which the Croatian DPA[38] also seems to follow when it emphasises that the right to the protection of personal data is not an absolute right and must rather be considered in the light of the current situation in its function in society. Also in the opinion of the German DPAs, the employer may ask and document whether an infection has been detected or contact has been made with a demonstrably infected person or the employee has been in a risk area. [39] Questions concerning the stay in a risk area or contact with infected persons are also considered to be allowed by the Latvian DPA.[40]

Although the Lithuanian DPA declares that employers may ask their employees about infection risks, symptoms or an existing diagnosis, the authority highlights that this right of access to information does not include a right to extensive documentation or the creation of data collections.[41] The Spanish DPA is against extensive questionnaires and in favour of a limitation to the question of symptoms and diagnosis according to the principle of data minimisation.[42]

Other DPAs are even more cautious about requests for information from employers. The French and the Belgian DPAs, for example, appeal to employers to (only) raise awareness and invite the employees to provide individual feedback of information concerning themselves in relation to possible exposure they had or to the competent health authorities.[43] Moreover, the employer could take possible preventive measures such as shifting to the home office or setting up communication channels that do not require the collection of health data. This is an aspect that the Hungarian DPA also addresses by stating that personal data should only be processed if other equally appropriate means do not promise success. The Hungarian DPA mentions, for example, specifying basic hygienic measures, cleaning work equipment and offices more thoroughly, providing disinfectants and requiring their more frequent use or regulating the order of receiving clients and using glass partitions at customer service desks, which may, in some cases, provide efficient solutions without the processing of personal data.[44]

The Finnish DPA points out a further interesting aspect in this context: an employee's health data may only be processed by people whose job description includes such processing. The employer must either designate such individuals in advance or specify the tasks that involve processing health data. Individuals who process health data are subject to a confidentiality obligation.[45] The Swedish DPA conversely limits this to access to such information: only employees where it is necessary should have access (only to the extent necessary) to information about other employees' (health) data.[46]

Beyond questions regarding the permissibility of the employer's information collection under data protection law, reference is made to the obligation of the employees themselves to report incidents. For example, many public authorities call for the widest possible (voluntary) participation of citizens because of their social responsibilities. The Spanish DPA goes even further. It bases the processing of data related to the coronavirus by the employer on the necessity to fulfil a legal obligation under Article 6 (1) (c) or Article 9 (2) in conjunction with the national provisions on the protection obligations of the employer. In doing so, it assigns the employees a duty to cooperate, who must provide all relevant information necessary for the assessment of required protective measures by the employer.[47] In Italy, too, workers and medical staff are seen as having a particular responsibility.[48]

37 Estonian DPA, Press release of 20 March 2020 <https://www.aki.ee/et/uudised/tootajate-isikuandmete-tootlemisest-koroonaviiruse-kontekstis>.

38 Croatian DPA, Press release of 18 March 2020 <https://azop.hr/aktualno/detaljnije/obrada-osobnih-podataka-o-zdravlju-u-kontekstu-izvanredne-situacije-izazvan>.

39 German DPAs, joint information paper on data protection and the Coronavirus pandemic, Press release of 13 March 2020 <https://www.bfdi.bund.de/DE/Datenschutz/Themen/Gesundheit_Soziales/GesundheitSozialesArtikel/Datenschutz-in-Corona-Pandemiehtml?nn=5217154>.

40 Latvian DPA, Press release of 17 March 2020 <https://www.dvi.gov.lv/lv/zinas/dvi-vers-uzmanibu-uz-personu-tiesibam-un-pienakumiem-datu-aizsardzibas-joma-veselibas-informacijas-konteksta/>.

41 Lithuanian DPA (n 17).

42 Spanish DPA, 'FAQ on Coronavirus' <https://www.aepd.es/sites/default/files/2020-03/FAQ-COVID_19.pdf>.

43 French DPA (n 32); Belgian DPA (n 23).

44 Hungarian DPA (n 26).

45 Finnish DPA, Press release of 12 March 2020 <https://tietosuoja.fi/en/artikkeli/-/asset_publisher/tietosuoja-ja-koronaviruksen-leviamisen-hillitseminen>.

46 n 21.

47 Spanish DPA (n 16) 3.

48 Italian DPA (n 25).

The Hungarian DPA even points out the criminal liability of those who knowingly infect others.[49]

b. Diagnostic Measures

The question of the admissibility of diagnostic measures, in particular screening tests, by the employer also causes many DPAs to be concerned. However, the views are very different. The main focus is on temperature measurement to assess whether employees or visitors have a fever, ie could be affected by an infection.

The French, Lithuanian and Luxembourgish DPAs are strongly opposed to these measures. [50] In this regard, in particular the Lithuanian DPA (as well as the Belgian and the Hungarian DPAs)[51] points out that this cannot be the duty of the employer, but has to be done by medical staff or health authorities.[52]

However, some DPAs make further distinctions: the Swedish DPA wants to ban systematic data collection, but points out that, for example, the 'whether' of the temperature measurement is not covered by data protection law, but only if these data are stored (which is 'normally' not allowed).[53] The Belgian DPA also appears to be of the opinion that the measurement of workers' temperatures is not necessarily a matter of data protection law, as it does not necessarily involve the processing of personal data.[54] The Austrian DPA, on the other hand, clearly states in its FAQs that even purely oral questions must respect the rules of the GDPR and that it does not matter whether the data collected in this way is also stored in physical form.[55]

The Slovak DPA takes a different approach by pointing out that such a type of data processing could be covered by Article 9(2)(i) GDPR in conjunction with the Slovak Act on Civil Protection of the Population No 42/1994[56] in the context of the emergency situation. This would require, however, that a public authority imposes appropriate protective measures on employers.[57] The approach from Hungary goes in a similar direction. The Hungarian DPA regards the requirement of screening tests with any diagnostic device (in particular, but not exclusively, with a thermometer) as disproportionate. Only if the employer has a justified suspicion of a possible infection or risk of infection (eg on the basis of information received from the employee) he or she may (only) call for tests to be carried out by health care professionals or under their professional responsibility and the employer is entitled to be informed only about the results of these examinations.[58]

Similar to its position on the completion of questionnaires, the Greek DPA does not want to exclude measures of the employer such as the 'calibration' of employees at the entrance to the workplace, at least not per se, by referring to the current critical times and highlighting the importance of respecting the principles of proportionality, data minimisation and adequacy.[59] Finally, the Bulgarian DPA must also see it in this way or similar, because it takes temperature measurements itself as measures of access control to the building of the authority, which both employees and visitors must undergo.[60]

4. Data Protection Implications in Home Office

Many Europeans currently work from home. In some countries, laws have even been enacted to regulate the ordering of home office by the employer.[61] Whether the employer may order home office is not a question of data protection law. However, how this is to be structured and whether the employer may

49 Hungarian DPA (n 26).

50 French DPA (n 32); Luxembourg DPA (n 23).

51 Belgian DPA (n 23); Hungarian DPA (n 26).

52 Lithuanian DPA (n 17).

53 n 21.

54 Belgian DPA, Press release of 13 March <https://www.autoriteprotectiondonnees.be/covid-19-et-traitement-de-donn%C3%A9es-%C3%A0-caract%C3%A8re-personnel-sur-le-lieu-de-travail>.

55 Austrian DPA, 'FAQ on data protection and coronavirus' <https://www.dsb.gv.at/documents/22758/23115/FAQ_zum_Thema_Datenschutz_und_Coronavirus_Covid-19.pdf/7cff6131-aed3-4bf5-8515-b724c82915a9>.

56 Act of the National Council of the Slovak Republic of 27 January 1994 on Civil Protection of the Population as worded in later amendments in the Act No. 222/1996 Coll., Act No. 117/1998 Coll., Act No. 252/2001 Coll., Act No. 416/2001 Coll., Act No. 261/2002 Coll. and Act No. 515/2003 Coll.

57 Slovak DPA, Press release of 13 March 2020 <https://dataprotection.gov.sk/uoou/sk/content/koronavirus-spracuvanie-osobnych-udajov-aktualizovane-1332020>.

58 Hungarian DPA (n 26).

59 n 15.

60 Bulgarian DPA, Press release of 13 March 2020 <https://bit.ly/39rB0cB>.

61 For example, Poland, Act of 2 March 2020 on extraordinary measures aimed at preventing, counteracting, and combating COVID-19 (7 March 2020) <http://dziennikustaw.gov.pl/D2020000037401.pdf>.

share the information that home office has been ordered for a particular employee with others also has implications under data protection law.

The technical facilities at home are often not designed for a protected working environment. In particular, technical and organisational measures (TOMs) for the protection of personal data are rarely taken, which the GDPR does not require for the 'private' processing of personal data, but does require for the 'professional' processing. Solutions are therefore needed that can be implemented quickly, but also safely. TOMs, which have been set up by the respective company, must also be observed in the home office.

In its Home Office Guide, the Polish DPA points out in particular that no additional applications and software may be installed that do not comply with the company's security procedures, operating and anti-virus software must be kept up to date, the personal devices must be locked when leaving the workplace, password protection is required and protective measures must be taken immediately if the device is lost. Emails should, if possible, only be sent via the business mail address, sender and recipient should always be checked critically, no links or files from unknown sources should be opened and encryption must be guaranteed.[62] The Danish DPA also emphasises that, where possible, employees should work on the company's own networks and management systems, which should only be accessed from home via secure VPNs[63]. If this is not possible in individual cases, it should be ensured that no one else (not even the own children) has access to the files and work devices and that the files are placed on the company's own system as soon as possible.[64] The Irish DPA also published some security remarks for securing devices, emails and cloud and network access, highlighting, however, that security issues must be observed while working 'analogue', too. Regarding paper records, steps should be taken to ensure the security and confidentiality of these records, such as by keeping them locked in a filing cabinet or drawer when not in use, disposing of them securely (eg shredding) when no longer needed, and making sure they are not left somewhere where they could be misplaced or stolen.[65] The Slovak DPA also declares the need for increased security measures while working via home office, but refers to the security recommendations of the National Cyber Security Centre SK-CERT for COVID-19.[66]

It is the Dutch DPA that goes into more detail on an aspect that is currently causing concern to many companies: the use of virtual services from third-party service providers such as e-mail, (video) conferencing, cloud, voice telephony and messenger services.[67] The Authority explicitly warns that such services, especially when offered free of charge, often collect a large amount of data, use it for their own commercial purposes and do not have sufficient implications to ensure data security. Consumer applications such as Facetime, Skype or Signal should therefore only be used with the necessary caution in exceptional cases, as, according to the Dutch DPA, '[i]n this crisis, good care takes precedence over privacy' but needs 'important precautions'. As a means of reducing risk, which anyone can take, the Authority mentions, for example, the deletion of chat histories after each communication, 'encrypted' communication in conferences by, for example, only mentioning customer numbers instead of names or agenda points instead of concrete information, as well as transparent handling of risks vis-à-vis discussion partners.

In order to prevent risks, according to the Austrian DPA, it is also permissible for employers to request and temporarily store the private mobile phone number of employees in order to be able to warn them at short notice about an infection in the company and so that they do not have to appear at the workplace. However, as employees cannot be forced to make this announcement and have to be duly informed about their rights, the Austrian DPA provides a sample form on its website for the collection of private contact data of employees for free use.[68] Collect-

62 Polish DPA, Protection of personal data in the case of distance working <https://uodo.gov.pl/pl/138/1459>.

63 In this regard also the Austrian DPA, 'Information sheet on data security and home office' <https://www.dsb.gv.at/documents/22758/23115/Informationsblatt_der_Datenschutzbehoerde_Datensicherheit_und_Home-Office.pdf/18c65716-537a-4a21-a835-f201428a9b98>.

64 Danish DPA, Press release of 16 March 2020 <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/gode-raad-om-hjemmearbejde/>.

65 Irish DPA, Press release of 12 March 2020 <https://www.dataprotection.ie/en/protecting-personal-data-when-working-remotely-0>.

66 Slovak DPA (n 57).

67 Dutch DPA, Press release of 18 March 2020 <https://autoriteitpersoonsgegevens.nl/nl/nieuws/veilig-thuiswerken-tijdens-de-coronacrisis>.

68 Austrian DPA, Press release of 17 March 2020 <https://www.dsb.gv.at/informationen-zum-coronavirus-covid-19->.

ing the mobile number is one thing, but passing this or other personal data to third parties is another. With regard to the naming of contact details for employees in the home office, the Swedish DPA clarifies that it is necessary to weigh up who receives 'private' contact details and that the reason why the employee is in the home office should be treated confidentially.[69] By the way: according to the Latvian DPA, if an employee does not follow the instruction to work in the home office, the employer is entitled to report the employee's data to the police.[70]

5. (Unsolicited) Government Contact via Electronic Communication

In many Member States, national legislation gives public authorities the right to contact citizens by electronic means in the event of a catastrophe. This is also the case in France.[71] Accordingly, many French people received a text message from the French government on 16th March with safety instructions in relation to Covid-19, but no data was transmitted to the government, the text was only forwarded via the telecommunications operators. In this context, the French DPA has made it clear that this procedure and the corresponding legal anchoring is justified in light of of Article 6(1)(c) to (e) GDPR.[72] The Slovenian DPA similarly cites Article 6(1)(e) GDPR as the legal basis for the text messages that Slovenian citizens received from their mobile operators on the instructions of the government's Communications Office and in which they were informed of restrictions on the right of assembly: according to Article 83 of the Slovenian Electronic Communications Act[73] telecommunications operators are obliged to implement government orders.[74]

The Lithuanian DPA further points out that this kind of contact with citizens is not to be regarded as direct marketing.[75]

6. Notification of Information about the Infection of a Person

The issue of the (public) announcement of an infection of (a) (certain) person(s), is an aspect that bothers many authorities. A distinction must be made between different cases: notification by health authorities, notification by employers to employees and finally journalistic reporting.

With regard to notifications by the competent health authorities, national DPAs broadly agree that legal bases have to be searched for in national law having been adopted to protect public and vital interests. Corresponding rules that set possibilities and limits to the processing of health data to combat pandemics have been set in national legislation. However and nevertheless, the DPAs highlight that special attention should be paid to the principle of proportionality and necessity in order to avoid stigmatisation of data subjects.[76] This could not only affect the economic and social situation of data subjects, but also have a counterproductive effect on the effective containment of the spread of the virus by preventing people from cooperating with employers and authorities for fear of stigmatisation. The Latvian DPA therefore also requires authorities to exercise careful judgement when disclosing information. For example, information on infected areas should be sufficiently broad to make it impossible to identify individuals (instead of the 200-soul community, the next largest city should be named).[77]

With regard to the disclosure of information by the employer it is again important to whom he or she wishes to communicate information. For example, national legislation (sometimes depending on the sector) often requires employees to report infections on their own initiative. Orders from the health authorities can also trigger such an obligation. With regard to the rights of employers to inform their employees about an infection of colleagues, the Finnish DPA clarifies that if an employee is diagnosed with COVID-19, the employer may not, as a rule, name the

69 n 20.

70 Latvian DPA, Press release of 20 March 2020 <https://www.dvi.gov.lv/lv/zinas/par-sensitivo-datu-publiskosanu/>.

71 Article L33-1 Code des postes et des communications électroniques as amended by Article 3 of Law no. 2019-1063 of 18 October 2019.

72 Press release of 19 March 2020 <https://www.cnil.fr/fr/le-gouvernement-sadresse-aux-francais-par-sms-le-cadre-legal-applicable>.

73 Official Gazette of the Republic of Slovenia, No. 109/12.

74 Slovenian DPA, Press release of 23 March 2020 <https://www.ip-rs.si/novice/obvescanje-drzavljanov-o-zacasni-prepovedi-javnega-zbiranja-preko-sms-sporocil-1175/>.

75 Lithuanian DPA (n 17).

76 Eg in this regard Greece (n 15)

77 Latvian DPA, Press release of 20 March 2020 <https://www.dvi.gov.lv/lv/zinas/par-sensitivo-datu-publiskosanu/>.

employee in question. The employer can (only) inform other employees of the infection or potential infection in general terms and instruct them to work from home. It should also not be possible to mention names if an employee is in quarantine.[78] According to the Swedish DPA it is basically possible to inform employees without mentioning their name that another employee may be infected. This is also the view of the Slovenian DPA, which argues that no personal data will be processed at all in this case. According to the Latvian DPA, the employer is not allowed to disclose any data to other employees.[79] The Austrian, Czech, German, Spanish, Swedish and the Belgian DPA agree as well that it should only be possible to mention names or other identifying information in exceptional cases.[80] The Slovakian DPA as well as the Irish DPA intend to leave the assessment of what is necessary in individual cases to the competent public health authority which is currently better able to assess what is necessary and appropriate to protect the health of the person concerned and the public.[81] Although the Danish DPA also wishes to limit naming to what is necessary in individual cases, it clarifies that it may well be necessary for the employer to inform management and colleagues that another employee has returned from a risk area, is in quarantine or is ill (without stating the reason) and, in individual cases, that an employee is infected with the coronavirus.[82] On the other hand, as regards disclosure of the name and health status of a natural person, the Romanian DPA generally emphasises (without explicitly excluding other possible justifications) that this can be done with the consent of the data subject.[83]

The Greek DPA points to an interesting aspect of the current data protection issues in relation to the coronavirus, which has, however, received little attention so far. It is about the media reporting on persons infected with the virus or differently formulated, the identifying reporting on corona patients. The public has a fundamental interest in knowing who is affected by an infection in order to be able to assess risks for their own health. The question arises, however, to what extent this can also justify identifying reporting, as this can lead in particular to social stigmatisation of the person affected. Therefore, according to the Greek DPA, the greatest possible use should be made of pseudonymisation and increased attention should be paid to technical and organisational protective measures (eg moving the data to a secure webspace where authorised parties can download it).[84] In this context, the Latvian authority makes a clear statement on the identifying postings on social networks by private individuals: this is clearly in violation of the rights of the data subject. Such information should only be given to the competent health authorities.[85]

III. Some Final Thoughts

What consequences the corona crisis will finally have for data protection is not yet foreseeable. In addition to the issues discussed in this report, other developments closely related to data protection issues have also played a role in recent days and weeks. For example, this is the case regarding websites that currently offer tools and advice on COVID-19 self-assessment, where users usually provide highly sensitive data on their health status. The Spanish DPA has already announced that it will initiate investigative measures and impose severe economic sanctions on rogue operators.[86] The Croatian DPA has also warned citizens against carelessly giving their data into the hands of such companies[87], while the Spanish DPA has issued a warning about phishing campaigns that exploit the uncertainties surrounding the coronavirus[88].

In any event, the overall picture of the notifications from the national DPAs currently seems to show

78 n 20.

79 Latvian DPA (n 40).

80 Austrian DPA (n 28); Swedish DPA (n 20); Belgian DPA (n 54); Spanish DPA (n 42); Czech DPA (n 14); German DPAs (n 39).

81 Slovenian DPA, Press release of 17 March 2020 <https://www.ip-rs.si/novice/obvescanje-v-primeru-pojava-virusa-med-ucenci-zaposlenimi-v-solah-in-vrtcih-1172/>; Irish DPA (n 35).

82 Danish DPA, Press release of 5 March 2020, <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/hvordan-er-det-med-gdpr-og-coronavirus/>.

83 Romanian DPA, Press release of 18 March 2020 <https://bit.ly/340aCph>.

84 n 15.

85 Latvian DPA (n 40).

86 Spanish DPA, Press release of 16 March 2020 <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-de-la-aepd-en-relacion-con-webs-y-apps-que-ofrecen>.

87 Croatian DPA, Press release of 20 March 2020 <https://azop.hr/aktualno/detaljnije/upozorenje-za-gradane>.

88 Spanish DPA, Press release of 12 March 2020 <https://www.aepd.es/es/prensa-y-comunicacion/blog/campanas-de-phishing-sobre-el-covid-19>.

two things in particular: on the one hand, the national DPAs are very keen to remove uncertainty and provide guidance by highlighting that data protection rules do not hinder health protection. The very fact that statements are issued on such a large scale by all DPAs is certainly a positive signal.

On the other hand, however, it is also apparent that the views of DPAs often diverge. This is certainly also due to the fact that the DPAs, like all of us, were surprised by the enormous impact of the crisis and therefore there was no room for finding a common line within the cooperation mechanisms provided for in the GDPR. In the area of tracking of location data, where there is a coordinated direction from the EDPB, the DPAs have been reluctant to provide their own guidance. It therefore remains to be seen and hoped that uniform EDPB guidance will also be published in other areas (as far as possible within the boundaries of the GDPR to each Member State within its margin of implementation), which will continue to ensure the consistent application of the GDPR in the European Union.

However, in the light of an overall view of the publications of national and European data protection authorities, it seems to be appropriate to conclude with one final remark: a decrease in the European level of data protection should be strictly avoided. Some reactions announced by the national DPAs are certainly understandable and correct in the light of the current situation. For example, many DPAs show understanding, for instance, on extended reaction times of data processors.[89] Moreover, none of the communications made any reference to the sanctions provided for by the GDPR in the event of non-compliance with data protection regulations. It is also right to stress that cooperation between individuals, businesses and public authorities (data protection and health) is more important than ever. It may also be appropriate to give health authorities greater scope for assessment because of their higher level of expertise in this regard.

However, if one reads between the lines in many explanations, it becomes clear that data protection is not seen so narrowly compared to (currently more important) health protection. The statements already mentioned above, that against the background of 'critical times' there must be possibilities for exceptions or that now is 'not the time to stubbornly exercise rights', are dangerous against the background of the fundamental right to privacy. This is particularly true because procedures once implemented are often difficult to reverse. Tracking location data can be cited as an example. If such procedures and mechanisms are implemented under time pressure, there is a risk that they will be reactivated in other contexts in the future. If we recall the situation regarding the retention of telecommunications data, which still concerns us today, we can get an idea where this will lead to. The EDPB and the EDPS also seem to recognise this risk, by continuing to look at the data protection implications of tracking location data, even though the data is 'actually' anonymised.[90]

We should fight the pandemic *but* protect civil rights and data protection.[91]

89 Dutch DPA, Press release of 20 March 2020 <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-organisaties-meer-tijd-vanwege-coronacrisis>; Irish DPA (n 35); the Portuguese DPA determined the interruption of the deadlines for responding to its draft resolutions, cf Resolution 2020/170 of 16 March 2020 <https://www.cnpd.pt/home/decisoes/Delib/DEL_2020_170.pdf>.

90 The EDPS even stated 'Moreover, the Commission should clearly define the dataset it wants to obtain and ensure transparency towards the public, to avoid any possible misunderstandings. I would appreciate if you could share with me a copy of the data model, once defined, for information' (n 11).

91 Cf on this the Appeal of the European Academy for Freedom of Information and Data Protection on 'Corona – Fight the pandemic, protect civil rights and data protection!' already signed by many experts <https://www.eaid-berlin.de/appeal-of-the-european-academy-for-freedom-of-information-and-data-protection-corona-fight-the-pandemic-protect-civil-rights-and-data-protection/>.