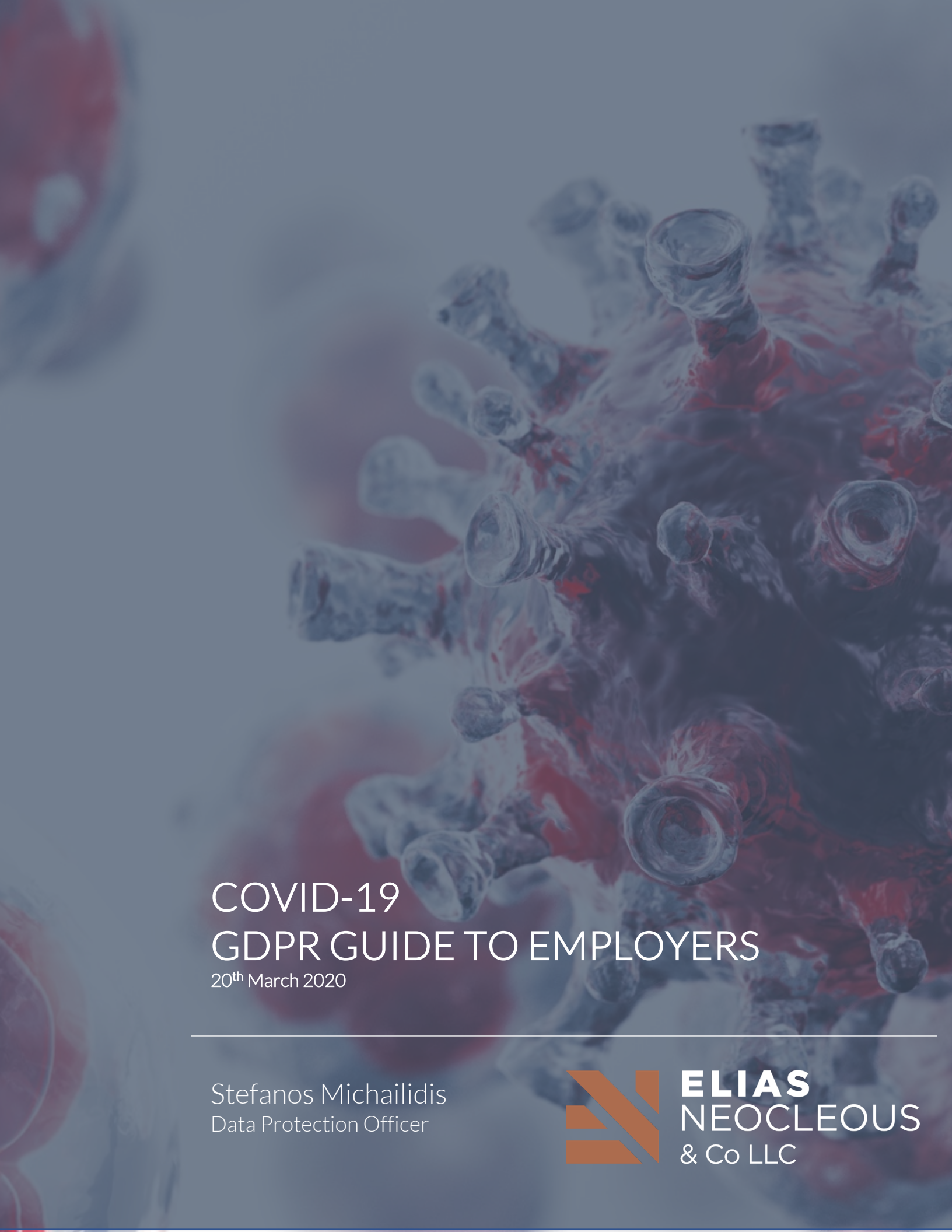

COVID-19
GDPR GUIDE TO EMPLOYERS

20th March 2020

Stefanos Michailidis
Data Protection Officer

ELIAS NEOCLEOUS & Co LLC

COVID-19 GDPR GUIDE TO EMPLOYERS

The outbreak of Covid-19 pandemic has forced governments to take measures that pose exceptional limitations to individual's rights and freedoms for the benefit of public safety. Companies on the other hand are asked to employ best practices in relation to hygiene and are asked to protect the workplace from health hazards, and for this, they are requesting the provision of certain personal information from their employees such as whether the employees have recently travelled, and in certain cases medical information such as symptoms and medical examinations which relate to the virus. However, do employers have a legal right to process such information which in ordinary circumstances would be a violation of the right of privacy of the employee.

Can medical data relating to the virus be processed by employers?

Information about symptoms of the virus are considered data concerning health and pursuant to The General Data Protection Regulation (EU) 2016/679 (the "GDPR" or "Regulation"), the processing of such data is prohibited as it falls under the "special category of personal data" unless one of the conditions of Article 9(2) apply.

Following the instructions of the European Board of Data Protection, it was stated that "Data protection rules (such as GDPR) do not hinder measures taken in the fight against the coronavirus pandemic and that companies could process data necessary for the employers for reasons of public interest in the area of public health or to protect vital interests (Art. 6 and 9 of the GDPR) or to comply with another legal obligation".

Initially, it was possible for business and organizations to rely on Article 6(1)(c) where processing is necessary for compliance with a legal obligation (duty to ensure the health, safety and welfare of employees – Safety and Health at Work Law 89(I) as amended (the "Safety and Health Law") and Article 6(1)(c) where processing is necessary for the performance of a task carried out in the public interest and in more rare cases Article 6(1)(d) protection of vital interests.

Whilst the above could justify processing of certain data, it does not allow the processing of special categories of personal data. For this, employers would need to consider Article 9(2)(b) which states that processing of special categories of data is allowed when it is necessary for the purposes of carrying out obligations of the employer in the field of employment. As explained above, pursuant to Article 13 of the Safety and Health Law, employers have the obligation to ensure the health, safety and welfare of their employees, and should take the necessary measures to achieve that. Therefore, it could be justifiable for businesses to request from their employee's certain data, in an effort to protect the employees and the workplace.

Furthermore, controllers could also rely on Recital 46 which offers guidance on the processing of information in instances where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. As per the Recital "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 epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters." Therefore, public interest and the vital interest of the data subject or of another natural person may constitute sufficient grounds for an employer to process medical data of its employees.

The role of employers in combating the Covid-19 virus.

Pending the issue of official guidance from the Office of the Commissioner of Personal Data Protection ("OCPDP"), useful guidance in relation to the role of employers in the response to the outbreak can be obtained from Data Protection Authorities across the EU, many of which have adopted varying approaches on how such information should be handled. The Spanish Agency for Data Protection has published a report which relates to the same matter and provides a lot of insightful information in relation to such processing. The Hellenic Data Protection Authority (the "HDPA") has taken a different approach, stating that the right to personal data protection is not absolute and it should be balanced with the fundamental rights and the right to life and health, whilst agreeing that the public interest and protection of employees health are sufficient grounds for the processing. On the other hand, the Italian Data Protection Authority said that Companies should refrain from "DIY" (Do It Yourself) data collection, but instead should act as dedicated channels of communication to the authorities of employees reporting symptoms. Furthermore, some useful guidance can also be sought from The Information Commissioners Office, the UK's Data Protection Commissioner (although not part of the EU anymore, following Brexit) stating that employers and organizations have an obligation to protect their staff and may need to ask their employees to provide certain information, such as if they have visited a particular country or if they have experienced coronavirus symptoms (click here and here for the guidance).Companies could also be asked to provide information about their employees to the authorities.

How should companies process medical data?

Businesses and organizations must understand that whilst they can request some information, the law is still the law. By gathering special categories of personal data, controllers carry a higher compliance burden, and adherence to the principles which relate to the processing of personal data pursuant to Articles 5, 6 and 9 is of paramount importance when processing such data. These principles should lie at the heart of every employer's approach to the processing of employee related personal data.

What information should companies request?

Companies must follow instructions and guidance provided by public authorities, bearing in mind the sensitivity of the information and the impact it has on the rights and freedoms of individuals. Information requested should be restricted to only what is strictly necessary and should be processed in a secure and confidential way.

How should the Company request that data?

Transparency and communication are essential. Employees should be informed that they are required to notify their employer if they travelled to certain countries or whether they or people close to them came in contact with a suspected case for reasons of workplace and public safety. Further, employers also need to inform their employees of confirmed cases of the virus, however that can be done in a way to protect the identity of the employee in question. Finally, employers should consider establishing a secure and confidential route or point of contact in relation to such reporting and ensure that access to that information is provided only to those on a strict "need-to-know" basis.

Data subject rights and the Commissioner?

Handling Data Subject Access Requests within the prescribed timeframe can be a challenging task during these tough times. Obviously, everyone's efforts and attention are focused on how to deal with this global crises and compliance with data protection regulation might not be up to par. Whether the OCPDP will take any action for resulting GDPR breaches and to what extent, remains to be seen.

The ICO has stated that they understand that resources, whether financial or human, might divert from their usual compliance routine or information governance work, and that they won't penalize organizations that need to prioritize other areas of work or adapt their usual approach during this period. Whilst the ICO cannot extend statutory timescales, it will inform people through their own communication channels that they might experience delays when making information requests.

Data breaches, prior consultation and data transfers

Business as usual. Companies should still ensure the integrity and security of their systems and data and should still notify to the relevant Data Protection Authority and data subjects any data breaches. The OCPDP should provide guidance as to whether deadlines for compliance will be extended or whether delays will be penalized.

Data transfers of special category of data should still be based on appropriate safeguards provided for in Article 46 of the Regulation or on binding corporate, rules provided for in Article 47 of the Regulation and the controller or the processor shall inform the OCPDP for the intended transfer before the said data are transferred.

Work from Home – Ensuring business continuity but care for Intellectual Property

During the pandemic, companies employ practices to ensure business continuity, such as "Work-From-Home" arrangements. Data protection is not a barrier to these different types of work. As per the Regulation, companies will simply need to ensure that they "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed"

Such measures include pseudonymization and encryption, ensuring the confidentiality, integrity and resilience of processing systems, providing the ability to store and access the data in a timely manner in case of incidents, and also guaranteeing that such measures are regularly tested to ensure and evaluate their effectiveness.

Whilst the Regulation does not provide guidelines on specific technologies to be used in an organization to achieve cybersecurity resilience, with the technologies currently existing, best practices to be followed when employees are working remotely is the use of a secured Virtual Private Network ("VPN") to connect to the Company's Firewall and network, with a two-factor authentication for logging in or some other measure with the same effect. Furthermore, companies should have in place endpoint security solutions such as endpoint detection and response ("EDR") and Next Generation Anti-Virus to protect for any malicious activity or breach. In relation to the intellectual property of any company, Data Leakage Prevention ("DLP") procedures and applications is a good practice to be implemented to have control of the company's documents.

Monitoring of emails

The OCPDP has previously provided guidance in relation to the monitoring of employee emails which would be allowed only if access is necessary for the proper functioning of the organization, the protection of the employer interests, property and managerial rights, the organization and management of a comparable task or project, work, and in particular expenditure control or for investigating possible offenses. Such processing should be pursuant to the additional requirements as explained in the guidance, including the adoption of a policy for such processing, and notification to employees in a clear and accessible manner amongst others.

This Guide is merely informative and is based on Ministerial orders, circulars and guidelines issued at the time of its publication and is not intended as legal advice in relation to any particular case.

For any further information or assistance with these, or your other fast-changing regulatory and legal obligations and requirements during these difficult times please contact Stefanos Michailidis or your usual contact at Elias Neocleous & Co LLC, or the Taskforce email.

Contact Us

ELIAS NEOCLEOUS & Co LLC

Elias Neocleous & Co. LLC, Neocleous House,
195 Makarios III Avenue 1-5th floor, Limassol,
CY, CY-3030, Cyprus,

+357 25110110

+357 25110001

info@neo.law

LegalTaskForce2020@neo.law