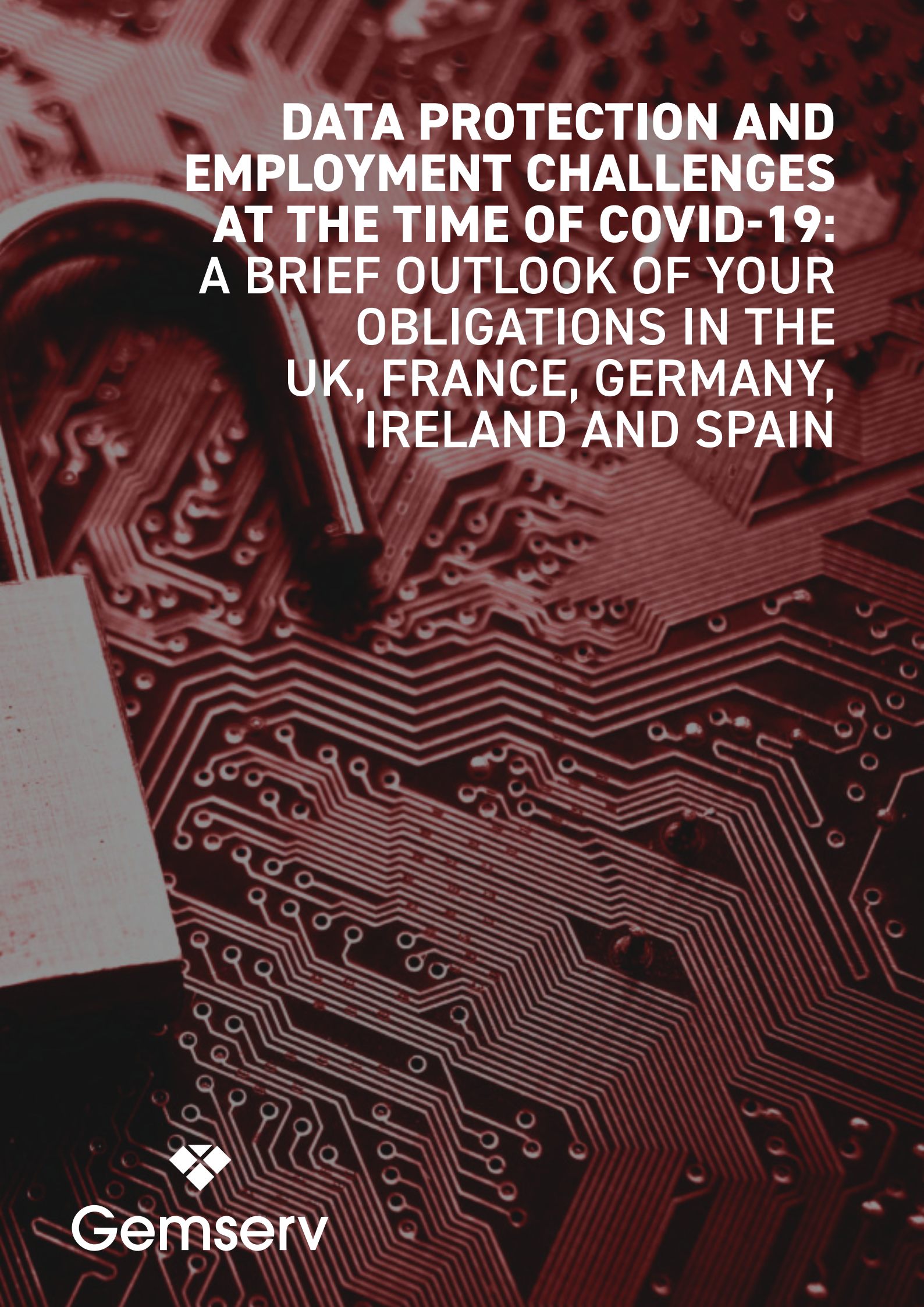

DATA PROTECTION AND EMPLOYMENT CHALLENGES AT THE TIME OF COVID-19: A BRIEF OUTLOOK OF YOUR OBLIGATIONS IN THE UK, FRANCE, GERMANY, IRELAND AND SPAIN

Gemserv

DATA PROTECTION AND EMPLOYMENT CHALLENGES AT THE TIME OF COVID-19

During these unique times, many organisations have switched to remote working and have to process health data from their staff. Employers are in the difficult position where they have to collect enough data to protect their workforce, whilst ensuring that they are not collecting the types of personal data that will put them in breach of the law. Additionally, having employees working from home raises challenges in monitoring staff performance and productivity. The rules around those two areas depend mainly on each country's local employment legislation, with the General Data Protection Regulation (GDPR) only as a guidance. In this paper, we will review and draw up a summary of the situation across the UK and a few European countries, France, Germany, Ireland and Spain.

PROCESSING STAFF HEALTH DATA IN THE CONTEXT OF COVID-19

In the context of COVID-19, companies may wish to collect information about their employees' health to facilitate the distribution of staff and resources (including those off sick), provide welfare benefits to entitled staff, and to prevent the spread of COVID-19 among staff. As health information is classed as special category personal data under the GDPR, its processing by employers is generally limited to specific situations, such as the legal obligation of employers (for instance, in the UK, under the Health and Safety at Work Act of 1974). As such, a focus on this such information is used in a privacy-friendly way will ensure only the relevant data is used effectively, whilst maintaining lawfulness and staff satisfaction.

GENERAL EMPLOYERS' OBLIGATIONS

In particular, companies may wish to collect information about an employee's fitness to work, either to facilitate the distribution of staff and resources, provide welfare benefits as applicable, and possibly to assess if an absence is genuine. However, the employer should bear several considerations in mind when collecting this data:

- Information may be needed to be collected for operational purposes, such as to facilitate the distribution of staff by calculating how long an employee may be off sick. Such information can be collected by the employer (e.g. their HR department) but should be limited to high-level reasons for sickness, the expected duration of the absence (whether or not COVID-19 related) and what adjustments the employee needs to have made to their working conditions. This should not include information on specific health conditions, unless it is required for the purposes below;
- Employers may need to collect information related to assessing staff eligibility for Statutory Sick Pay (in the UK, and its equivalent in other European countries), for those who are self-isolating due to COVID-19, or forced to isolate due to their vulnerability. However, employers should only collect the information relevant to the employees' health conditions, including COVID-19 symptoms or information on vulnerability. If an assessment is needed (e.g. beyond the 7-day Statutory Sick Pay period in the UK), then a doctor or healthcare provider should be used.
- Employers may also want to support employees with issues such as mental health difficulties related to working from home, to help protect employee wellbeing. In this circumstance, for data not directly related to COVID-19, an occupational health provider should be used where possible to collect information on employees' conditions.

To collect such information, employers should use an occupational health provider if one is available. If such a provider is not available, data should be collected from the employee by the company's HR department. Some jurisdictions, such as the Netherlands and France, absolutely require employers to use an occupational health provider to collect information related to medical conditions. If there is a need for sick pay or working adjustments, the health provider will advise the company.

DATA PROTECTION AND EMPLOYMENT CHALLENGES AT THE TIME OF COVID-19

OBLIGATIONS FOR COVID-19 CASES AND INFECTIONS

Separately, employers may have a legal obligation to report COVID-19 cases if there is reasonable evidence that exposure occurred at work (for example in the UK, under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013), in which case, further information about symptoms and incidents may be collected from employees.

In most European countries, collecting information about employees' potential COVID-19 symptoms may be necessary to identify whether the disease has been transmitted in the workplace. However, this should be limited to collecting data (such as symptoms, travel information, location and other staff they've come into contact with) from known or reasonably suspected cases, and should not collect detailed data on symptoms or attempt a diagnosis (which should be left to health providers). A good method to achieve this would be to advise employees to notify the company if they suspect, or are diagnosed with, COVID-19, rather than assessing all employees by default.

In addition, employers may be able to process personal data of employees for reasons of substantial public interest, given the public emergencies that have been declared with respect to COVID-19. Employers should monitor the specific legal obligations with respect to reporting or data collection and make a proportionate decision on what extra data (e.g. around staff location, movement, or symptoms) can be collected.

Nevertheless, some jurisdictions, such as the Netherlands and France, have again been more stringent. The Netherlands prevents any personal data being generally collected by the employer from employees about COVID-19. This data should be collected via the occupational health provider. In France, employers can only process limited data about the identity of employees who believe they have symptoms or are diagnosed with COVID-19.

As such, taking into account the local guidance, organisations should develop a plan outlining which data may need to be collected in the situations above and what controls (in particular data minimisation, purpose limitation, and limitations of access to relevant staff) will be introduced.

Data minimisation and proportionality is key for most countries. You can collect data on symptoms and travel history, require your employees to notify if they are diagnosed with COVID-19, record who is infected and notify staff, but with some limits.

Firstly, on symptoms, in the UK and Germany employers are allowed to collect data as long it is proportionate. In Ireland and Spain, the collection can only occur on the existence of symptoms, and employers should refrain from recording the actual detailed symptoms. In France, the collection must not be systematic and general across all staff, and only individuals affected must be recorded. Most countries also require employers to limit collection on their employees' travel history to areas of risk and for the incubation period. However, in France, such data is considered as private and employers cannot require their employees to disclose this information.

Employers may require their employees to notify if they are diagnosed with COVID-19 (in some instances, employees even have a duty to inform) and record who is affected amongst their staff. Such approach is generally acceptable in all countries, but in France this should be limited to the identity of the employee and the measures taken after the notification.

It is interesting to note that in all countries notifying the rest of the staff of someone's diagnosis is allowed under particular circumstances. The identity can be disclosed where it is strictly necessary to contain the spread of the virus, it cannot be a general announcement and only staff who have been exposed should be informed. Information on the health condition of the employee should remain confidential at all times. Finally, public authorities should be notified as required, as data protection laws do not prevent reporting of COVID-19 cases where such information is necessary to safeguard public health.

Gemserv

DATA PROTECTION AND EMPLOYMENT CHALLENGES AT THE TIME OF COVID-19

EMPLOYEE MONITORING WITH A WORKFORCE WORKING REMOTELY

Usually, the most acute challenge for organisations in respect of employee monitoring is CCTV. At a time where most, if not all of an organisation's staff is working remotely, safeguarding the organisation's network and information is essential. This requires monitoring the company's traffic and devices remotely, which can also be used to monitor your employees' productivity and performance.

The general rule in Europe around employee monitoring is that their privacy should be respected and that any monitoring should be proportionate to the purpose, but the rules vary a lot depending on the countries.

IN THE UNITED KINGDOM

In the UK, an employer can monitor its staff emails and networks for the following purposes:

- To establish the existence of facts or demonstrate compliance with regulatory practices or procedures relevant to the business, and to demonstrate standards to be achieved by persons using the company's IT, such as quality assurance and training;
- To prevent or detect fraud;
- To detect or investigate unauthorised use or ensure the effective operation of the company's IT.

The use of highly invasive technologies such as mouse-movement tracking, keylogging or screen recording to monitor employees is not lawful.

IN FRANCE

In France, the use of email in the workplace is presumed to be professional, but emails that are flagged 'private' in their subject line or stored in a folder named 'private' are considered private correspondence and cannot be accessed by the employer without notifying the employee. It is accepted that an employer can monitor its staff emails and networks for the following purposes:

- Training;
- Assessment or appraisal;
- Improvement of the quality of the service;
- Detection of fraud;
- Follow-up of the accomplishment of an employee's duties.

IN IRELAND

The Data Protection Commission does not issue specific guidance on employee monitoring. Traffic and devices monitoring should still comply with the GDPR principles such as necessity, legitimacy, proportionality, transparency and data minimisation. A few case laws have been ruled towards this direction in the past in Republic of Ireland, so the obligations of a controller remain significant, although perhaps less formalised.

IN SPAIN

In Spain, employers can access content derived from the use of devices made available to employees for the sole purpose of monitoring compliance with work or statutory obligations and ensuring the integrity of such devices. Acceptable use of the employer's device must be determined in advance and employees must be informed.

IN GERMANY

In Germany, private emails are subject to the secrecy of telecommunications and must not be monitored by the employer. Therefore, there is a substantial risk when employers allow private use of their IT by employees for private purposes. Some recommended to completely prohibit the private use of the company's IT to prevent any criminal law liability resulting from breaches of the secrecy of telecommunications. A workaround is to clearly ask employees to flag private emails as private and store them separately from business emails.

Employers can monitor employees' devices and communications in the following circumstances:

- Preventively discourage employees from committing criminal offences or other breaches of duty in the employment relationship and performing the employer's duty of care towards employees;
- Uncovering possible breaches of duty in the employment relationship;
- Investigating fact-based suspicion of criminal offences;
- Controlling an employee's work performance;
- Proving an employee's misconduct for disciplinary measures;
- Protecting the company's property and rights;
- Complying with legal obligations.

Navigating this period is not easy for many organisations, but even with some differences between countries, the principles remain the same: data minimisation and proportionality are the keywords when processing health data or monitoring your employees.

Gemserv

Gemserv

LONDON

+44 (0)20 7090 1022

bd@gemserv.com

IRELAND

+353 (0)1 669 4630

ireland@gemserv.com

CONTACT US TODAY, TO DISCOVER HOW WE CAN HELP YOU