

# THE BYWORD

MONITORING IN THE WORKPLACE

04

Monitoring in the workplace

06

Data privacy awareness versus emerging tech 09

Monitoring outside work



# CONTENTS

# 04

Monitoring in the Workplace: An international perspective on a changing environment

# 10

The case for monitoring – how the courts are responding

# 05

Key findings

# 12

Benefits to employees – are there benefits to new types of monitoring for employees?

# 06

Data privacy awareness versus emerging tech

# 13

Conclusions

# 07

How is the law coping with data protection concerns about monitoring?

# 14

Contacts

# 08

What are the main restrictions on workplace monitoring?

# 09

Monitoring outside work

# MONITORING IN THE WORKPLACE

# An international perspective on a changing environment

echnological advances are helping many employers to monitor their workforce in increasingly sophisticated ways, whilst at the same time, public attitudes towards individual data privacy are hardening. Two important drivers of these changes came to a head in 2018 – the advent of the General Data Protection Regulation (GDPR) in Europe and the public's changing perception towards the way certain social media outlets, such as Facebook, handle privacy.

The effects of these developments are coming into sharp focus in workplaces worldwide with indications that employees are becoming less likely to accept unwarranted or unexplained intrusions than ever before. Our research analyses the rules on monitoring in the workplace in 41 countries and examines how the law is coping with the growing tensions between new technologies and the strengthening of privacy rights.







Employees are becoming less likely to accept unwarranted or unexplained intrusions than ever before

- » There are differences in workplace monitoring rules in different parts of the world. Even within the EU GDPR bloc, there are noticeable variations that employers need to take into account.
- » In terms of restrictions on workplace monitoring, the general rules are that employers must tell their employees if they are going to be monitored and must do so before the monitoring starts. Employers must also have a legitimate interest to monitor, which is balanced against the rights and freedoms of employees. The direct consent of the employee is not needed everywhere, but in some places it is, and so it is important to know the local rules.
- » Employers need clear reasons to monitor employees outside of working hours, and it should be kept to the minimum level necessary to achieve their aims. It is far harder to justify than monitoring within working hours just about everywhere.

- » There is no substitute for having a good, clear policy about monitoring. It is also beneficial to set clear parameters for use of employer-owned devices for personal reasons and for the use of social media. The courts can come down heavily on those without a policy.
- » We see an emerging trend in some countries towards using new tech for the benefit of employees' health and wellbeing. But in many places employers need the specific consent of employees to do this, and in some countries, employers must avoid collecting or processing any health data that is generated. The best solution to this problem is to outsource this function to a suitable third party.

#### COUNTRIES TAKING PART IN OUR RESEARCH:

Argentina, Austria, Belarus, Belgium, Brazil, Bulgaria, Canada, Chile, China, Colombia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, Ireland, Israel, Italy, Japan, Latvia, Luxembourg, Mexico, Netherlands, New Zealand, Panama, Peru, Poland, Romania, Serbia, Singapore, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States.



# DATA PRIVACY AWARENESS VERSUS EMERGING TECH

ver the last couple of years, global awareness of data privacy issues has grown immensely, in a way that impacts the workplace. In Denmark, for example, employees are increasingly interested in what data their employers hold about them. In Hong Kong, there is an increase in data access requests from employees, indicating growing awareness of their rights. The same is true in many larger EU countries, but also in smaller ones, such as the Czech Republic, Romania and Hungary. In Poland, although employees are used to having their emails and internet usage monitored, any more 'invasive' form of monitoring (such as biotech) would likely be questioned. In Cyprus, the advent of the GDPR has raised awareness, put privacy on board agendas and changed the attitudes of employers to employees' privacy rights as a whole.

In the UK, the GDPR has raised the risk profile and general awareness of privacy rights, but the fundamental approach to monitoring remains the same. When monitoring employees, employers need to consider data protection law, human rights law, and specific monitoring legislation.

All over the world, the challenge is to balance the possibilities offered by new types of technology with individual data privacy rights. Some countries are more at the sharp end of tech developments than others. In Germany, several employers have suffered ransomware attacks, forcing employers to increase data protection and establish suitable compliance and monitoring mechanisms.

Other countries are more concerned with accommodating a shift in employee working habits.

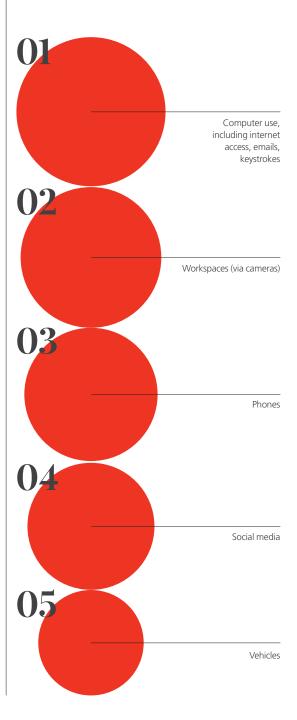
In Ireland and Italy, we see a trend towards 'bring your own device' (BYOD), involving employers in introducing BYOD policies to manage how employees connect to their networks. The challenge for employers is essentially to work out how to monitor personal devices used for work in the same way as they monitor company devices. In Italy, a consensus on how employers should do this is yet to be reached.

In the Netherlands, more and more employees are working from home and this again leads employers to want to monitor productive activity. Technology is starting to enable this, with wearable tech, GPS trackers etc., but balancing these developments with privacy is proving a challenge.

In France, the hottest topic is arguably biometrics. The Data Protection Authority (the CNIL) has just issued a new regulation – which is stricter than the GDPR: the purposes for which employers can use biometrics are strictly limited, as are the type of biometrics they can use. For example, biological sampling (e.g. of saliva or blood) is prohibited. Iris, fingerprint and hand veins, for example, can be used, but the employer must justify why they are using them, including the reason for using one feature over another.

Interestingly, clocking on is an issue in Switzerland too, but from the opposite angle: the authorities are stepping up checks to ensure employers comply with their duty to record hours worked by employees and in consequence, employers are using ever-more sophisticated means of clocking people in and out (e.g. voice, finger prints and facial recognition) – and that seems to be accepted by workers, for now at least.

WHAT TYPES OF MONITORING DO EMPLOYERS MOST OFTEN ENGAGE IN?



# 07

# HOW IS THE LAW COPING WITH DATA PROTECTION CONCERNS ABOUT MONITORING?

# Does the law provide certainty?

onitoring is often regulated via general data privacy law, to which some countries add specific labour law provisions. Others rely on their constitutions, international human rights treaties and conventions covering fundamental rights to privacy. Others still look to case law, ministerial guidelines and best practice.

In terms of coping, most of the GDPR countries say they are confident for the moment that the law protects individuals and provides clarity for employers. Some, such as Finland, France, Germany, Denmark, Italy, Austria and Ireland, had strong legal protection before the GDPR, but the GDPR has focussed Europe's attention on privacy as never before. In this, the UK is somewhere between a continental European approach and a more employer-friendly US approach.

But it is noticeable that although the EU may look like one bloc, many GDPR countries still have their own particular preoccupations – and points to note for international employers. In Finland, employers can only process personal data that is directly necessary for the employment relationship, meaning that not all monitoring activities are permitted, regardless of the employer's interests or the level of information given to employees. Spain is gradually introducing more limits on monitoring as a way of slowing the implementation of some technologies - particularly those that capture sensitive data. Meanwhile, the Netherlands

has two conflicting data privacy provisions relating to health data, one saying employers must have information about drug and alcohol abuse to dismiss someone for this, the other saying it is unlawful to process employee health data of any kind. Employers need to beware of this trap.

It is worth noting that on the edges of Europe, various countries are implementing something similar to the GDPR. In Turkey, a new law came into force in 2018 and society more generally has been taking much more notice of privacy issues than ever before. Belarus is also about to adopt its first data protection law and it is expected that this will offer employers some clarity on workplace privacy issues too.

A new privacy law has just been approved in Brazil and employers are adjusting their policies to address the long tradition of permitting private use of corporate email, as this results in an entanglement of professional and private data. The law is tightening in Chile too, where an amendment should provide for a data protection agency to oversee compliance.

The US and Canada have something of a patchwork of law on data privacy, which makes those countries all the harder for employers to navigate. The law in the US involves state, federal and case law and there is no single blanket piece of legislation. Yet some of the biggest technological innovations come from the US and so some sort of reaction at a federal level can be expected as society becomes increasingly cognisant of privacy issues.

The law of privacy in New Zealand has not changed in over 25 years and its principles can be interpreted to cover monitoring using the full range of modern technology. The basic legal requirement that employees must be told when information is being collected about them still holds true.

By contrast, in a number of countries the law is not as robust as it should be. In China, there were several high-profile disclosures of private information last year and people are starting to pay close attention to privacy issues for themselves and their families. Our lawyers comment that data protection law in China is not yet robust enough, for example, there are no restrictions on workplace monitoring. In Hong Kong, the Privacy Commissioner has said several times that the law lags behind other countries, especially post-GDPR, and his department has therefore started a review. Proposed changes should emerge soon. In Singapore there is now a greater awareness of the issues, but the law still lags behind. In Mexico, there is both a lack of law and lack of clarity, making it hard for employers to know the parameters. In Colombia, much is still left to selfregulation and there is an urgent need for rules that deal with new ways of working – including rules to define what kind of monitoring is acceptable. In Israel, a consolidation of data protection law is needed, given the continual march of technology.

Some countries would like change, but it is not happening yet. This is the case in Japan, where monitoring is decided on a case-by-case (and not very transparent) basis and in Panama, where employers are under no obligation to disclose what they monitor.

Finally, quite a number of jurisdictions lament that there is nothing specific in their law on workplace monitoring. Of those surveyed, our lawyers in Bulgaria, Serbia, Estonia, Sweden, Hungary, Latvia, Brazil and Peru all felt this creates uncertainty for employers.



# WHAT ARE THE MAIN RESTRICTIONS ON WORKPLACE MONITORING?

The rise of remote or flexible working is putting pressure on employers to keep track of their staff

TOP REASONS EMPLOYERS GIVE FOR MONITORING EMPLOYEES

O1 Protect confidential information and trade secrets 02 Performance 03 Protect from external threats of violence Track productivity Prevent theft ()5(both internal and external) 06 Comply with employment policies, such as prohibitions of harassment

ore and more people are working from home, working on personal devices, sometimes using work devices for personal reasons, and as a result, their work and personal lives are becoming more entwined. But there is a basic business need for employers to be able to monitor what is happening in this complex picture.

The largest block of countries with similar rules on monitoring is the EU. Under the GDPR, employees have an expectation of privacy that would be at odds with extensive monitoring in the workplace. The transparency principle in the GDPR requires that employers must tell their employees if they are going to be monitored and must do so beforehand, but specific consent is not required - although it is worth noting that in some countries, such as Austria, monitoring is generally only possible with the agreement of the works council. Monitoring should be based on the legitimate interests of the employer, as weighed against the rights and freedoms of employees in a 'balancing test'.

As it turns out, many other places also have rules that are reasonably similar to this. In Argentina, for example, if employers want to monitor emails, they must have a proper policy in place and employees must be notified beforehand that they have no expectation of privacy whilst using the employers' devices for private purposes. In Brazil, the labour courts have long accepted the employer's right to monitor emails

and internet use, although Brazil's new law may lead the courts to impose new conditions. In Hong Kong, employees have no expectation of privacy when using company equipment and software and monitoring is largely accepted by employees.

In Canada, employees retain some expectation of privacy in the workplace and whilst using employer devices. But their privacy rights are not absolute as they can be balanced against the employer's legitimate business interests.

In the US, the picture is more complicated, and employers sometimes end up in court trying to defend monitoring by trying to show that the employee had no reasonable expectation of privacy. The advice our lawyers give employers is to have their employees acknowledge in writing, in advance, that they understand their communications will be monitored. It is also preferential to have clear policies, to head off any expectation of privacy.

Most legal regimes stop short of requiring employee consent to monitoring but in China, the rules are that if an employer wishes to monitor employees it needs to disclose this and obtain their consent in advance. It must also let the employee know the reasons for the monitoring and the scope of it. Information collected can only be for employment-related purposes and needs to be kept securely.

In Japan, it is good practice to notify employees in advance about monitoring, but monitoring seems to be socially accepted within the workplace and there is little pushback for the moment.



# MONITORING OUTSIDE WORK

# When is it ok to monitor outside the workplace?

he general rule of thumb almost everywhere you go is that it is much harder to justify monitoring outside working time. Therefore, employers should avoid doing this unless they have a very good reason.

We found that in Panama, Colombia and Mexico, monitoring outside working hours would normally be considered excessive. Similarly, in Peru, monitoring of employees outside working hours is a privacy violation. In Argentina, what an employee does outside work is up to them, and no disciplinary action is possible. The story is similar in China. In the Czech Republic employees would take a dim view of monitoring outside work and neither is it accepted in Finland, Hungary, Cyprus, Austria or Bulgaria. In Estonia, a GDPR country, monitoring can only be done for work-related activities and employers cannot read private emails of employees sent using their business email address.

In Latvia, monitoring employees outside working hours is not usually legitimate, but exceptions are possible if there is strong suspicion of wrongdoing by an employee. Romania's rules are that the employer needs a proven legitimate interest to monitor employees either outside working hours or at other locations, and that is hard to find. The same pattern is found in Turkey, New Zealand and Switzerland. In the Netherlands, monitoring outside working hours is usually not possible because it would be hard to support it with a legitimate interest.

In Denmark, one test is how intrusive the monitoring is compared to the issue it is intended to address. For example, employers cannot monitor vehicles made available for employees' private use on weekends and during holidays. In Poland, the monitoring of employees outside working hours would have to be justified case by case.

In some countries, the emphasis is slightly different. Our lawyers

in Belgium confirm that as long as the monitoring is related to work, the same rules apply as to monitoring in the workplace.

There is a similar approach in Canada and Greece, where there is no fundamental legal difference between monitoring at the workplace and elsewhere; it is simply a question of proportionality. In Italy, monitoring outside work falls within a different set of rules and in such cases, employees are no more protected than the general public.

In Germany, again, monitoring outside of working hours or outside the workplace is generally a breach of privacy, but in an interesting twist, employers are starting to support employees by using technology to block calls and emails at certain times outside working hours to support their 'right to be unavailable'.



# It is much harder to justify monitoring outside working time

#### TYPES OF TECHNOLOGY MOST OFTEN USED BY EMPLOYERS TO MONITOR EMPLOYEES



# THE CASE FOR MONITORING

How the courts are responding to the use of new technology for monitoring



ost of new technological advancements we are seeing consist of different

ways to monitor employees, but some cases before the courts are also about how employees use social media, and whether posts that are harmful to the employer can be sanctioned.

# MONITORING USING TECHNOLOGY

Some countries are far stricter than others in terms of their rules about monitoring. At one end of the scale, in Germany, if an employer simply wants to introduce Microsoft Office into a workplace, the works council can decide to block it, leading to a special conciliation procedure. Apparently, the problem is it could be used to monitor employee performance, if only by manually adding performance data. Other countries are much more permissive, but it can depend on the kind of technology involved. – for instance, Japan, where monitoring by the employer seems



to be much more accepted.

But it can depend on what the technology is – as discussed below.

#### SURVEILLANCE CAMERAS

The judgments coming out across the globe on camera surveillance show a mixed picture, but it is still possible to discern a pattern. The courts are generally unlikely to say continuous, intrusive or unannounced camera surveillance is allowed and there need to be good reasons to persuade them otherwise.

However, in Canada, in a Quebec case, they did just that. The court found the installation of five surveillance cameras that continuously monitored employees at a meat processing plant permissible. Although the continuous surveillance was a prima facie breach of the Québec Charter of Human Rights and Freedoms, the employer had reasonable grounds for it. The employer had recently lost a major customer as a result of a contamination incident and so the purpose of the surveillance was to discover its source, rather than to monitor the employees.

Similarly, in Germany, an employer used open video surveillance at its public salesrooms and cash desks and saved all records for several months. Based on a concrete suspicion, the employer analysed the material and discovered an employee had stolen money six months previously. It dismissed the employee and the courts decided the records should not be used in evidence, as they had been stored for an excessively long time. But rather surprisingly, the Federal Labour Court overturned this judgment and allowed the records in evidence, saying the suspicion of a crime overrides data deletion obligations. This begs the question:

what about all the records stored over several months that did not show any crimes? The Federal Labour Court indicated that some employees may have a claim for damages in prospect as a result.

In Greece in 2015, the Hellenic Data Protection Authority fined a company for placing a camera in a management office, which was found to be disproportionate. In a case in 2017, the Authority found cameras in company truck illegal. The cameras were put in for the safety of drivers, cargo and other individuals, but each lorry had two - one constantly recording the route and the other continually recording the driver.

A recent Spanish case found that a noticeable sign at the workplace informing people about cameras was not enough: the employee representatives also needed to be specifically informed – and the need to involve them seems to be a growing trend.

The Dutch Supreme Court decided in 2001 that employers needed a 'serious interest' if they wanted to use hidden cameras and that they should be used only as a last resort. This stance has provoked much case law, most recently a case in which the employer had put mystery shoppers in its shops to film employees. When the employer showed the video images to the employees as part of discussions about performance, the case ended up in the courts – and was found to be an infringement of privacy law.

#### LOCATION TRACKING

Location tracking is another area of technological growth that raises privacy concerns. In Hungary, in a key case in 2014, the Supreme Court ruled it was forbidden to track the location of employees without informing them first. The employee resigned



without notice when he realised that his employer had activated the location tracking system on his company mobile phone without his knowledge. The employer did not prohibit private use of the phone and so the employee used it outside of working hours – and as a result, the employer could find out where he was at any time of night or day.

Tracking outside working hours is not a good bet in the US either: in a case in 2013, the High Court for the State of New York held that the employer was entitled to use GPS on an employee's private vehicle, as part of an investigation into the employee's suspected misconduct. However, because the employer had monitored the employee whilst off-duty as well, it had gone beyond what was reasonable. Therefore, the employer could not use any of the evidence obtained by it in the dismissal hearing. Our US attorneys recommend employers use applications that automatically switch off when an employee clocks off

By contrast, in Luxembourg, the Court of Appeal ruled in a case in 2017 that an employer was able to keep geolocation tracking activated on a vehicle exclusively reserved for professional purposes outside working hours - and use the evidence obtained by it in Court.

#### KEYLOGGER SOFTWARE

Software that logs all keystrokes made by employees is available for employers to purchase, but it's worth noting that in many countries, it is considered a step too far. For example, an employer in Germany made it quite clear to its employees that it intended to install keylogging software. The employer found out, with the help of the software that one employee was doing an excessive amount of private business during work. However, the Federal Labour Court decided that the keylog data could not be used as evidence because the employer had no concrete reason for monitoring its employees so comprehensively.

#### **BIOMETRICS**

Biometric data is increasingly used to enable employees to clock on and off at the workplace. But the sensitivity of this data gives some countries cause for concern. For example, in Israel, in the case of Qalansawe, the court found against the employer for requiring employees to clock on using fingerprints.

Meanwhile, the French Data Protection Authority recently imposed a EUR 10,000 fine on a company that monitored its employees using fingerprint recognition. It failed to show exceptional circumstances requiring the use of biometrics, making it unlawful.

#### USE OF SOCIAL MEDIA

There is no shortage of cases from around the world involving posts on Facebook as the courts grapple with whether employees can legitimately be dismissed for reputationally damaging posts. In many countries, the issue turns on what is private and what is public. In France, comments by employees on Facebook are generally considered private and are protected under freedom of expression – but this is only if the posts are made to a 'private' circle of 'friends'. If an employee defames the employer publicly, this can lead to dismissal.

In New Zealand, an interesting case from 2015 (Hammond - v -Credit Union Baywide) reverses the focus by considering what happens when the employer tracks private posts and then goes on to misuse them. Ms Hammond was dismissed from Credit Union Baywide and later held a small function where she served a cake, iced with an expletive towards Credit Union Baywide. She posted a photo of the cake on Facebook, accessible only by her Facebook 'friends'. Credit Union Baywide heard about it and asked a current employee who was a Facebook friend, to access it for them. They then distributed the photo to other potential employers to ensure



she wouldn't get another job. Ms Hammond took out a breach of privacy claim and was awarded record damages of NZD 168,070 (approximately EUR 100,000).

One key to managing risk is to have a clear, suitable and effective policy. In Ireland, an employee was awarded EUR 7,000 to compensate for his suspension for alleged gross misconduct. The employee had posted negative comments about his employer on social media - but crucially, the employer had no social media policy.

One key to managing risk is to have a clear, suitable and effective policy. In Ireland, an employee was awarded EUR 7,000 to compensate for his suspension for alleged gross misconduct. The employee had posted negative comments about his employer on social media - but crucially, the employer had no social media policy.



An employee resigned when he realised his employer had activated location tracking on his company mobile phone without his knowledge

# BENEFITS TO EMPLOYEES ARE THERE BENEFITS TO NEW TYPES OF MONITORING FOR EMPLOYEES?

onitoring should not all be about 'Big Brother'
– some new types of monitoring are being developed to help to reduce stress and improve the health of employees. This should be a positive development, as it may increase productivity in the long run.

However, many countries have not evolved in this way yet. This is the case in Belarus, Cyprus, Denmark, Estonia, Greece, Japan, Latvia, Mexico, Panama, Peru, Romania, Serbia, Singapore, Switzerland, Turkey and – interestingly – also in the US.

But it is the opposite in Italy, where new tech is increasingly used to organise work - and this is generally acceptable as long as employers comply with a specific tech and monitoring reform made in 2015, plus the GDPR.

In some countries, although these types of technology may be new, the concept of employers being responsible for providing a healthy working environment is enshrined in health & safety law and is therefore already an obligation. This is an interesting twist, as it is effectively the reverse of the prohibitive stance of data protection law: employers are required to monitor in some circumstances and the focus is on how to use technology to do this more effectively. This is the case in Argentina, Colombia, Cyprus, Germany, Greece, Romania and Turkey.

In Bulgaria and Sweden, workers in potentially dangerous working conditions are monitored for health and safety reasons, though in more run-of-the-mill working environments this would be unlawful. In a number of countries drug and alcohol testing is routinely done as part of ensuring a safe environment for all workers.

In various countries, people with certain jobs, such as pilots, are routinely health-checked. Other employees are closely monitored to ensure they don't go over the maximum time they can lawfully work and that they take their breaks. Recently however, a company in Germany implemented a system that generates data about how time is spent to help management distribute work more evenly. But as this could also be used as a performance-monitoring tool, the Court ordered it to be switched off.

In New Zealand, the legal requirement for a healthy work experience often leads to monitoring and some larger companies invest in general health monitoring. But the key here is to obtain employee consent. In Belgium, monitoring, say, heart rates and blood pressure, would likely be prohibited, as too intrusive. The key, again, could be consent, although it may not be valid unless there are clear advantages for the employee.

But in some countries, the best way of enabling health monitoring is by the employer keeping well away. In France, occupational health services do regular medical checks on employees, but those services also handle all sensitive health information, keeping it at one remove from the employer. The position in Finland

is analogous, as employers may offer employees the means to measure health data, but because employers can only process what is strictly necessary for the employment relationship, the employer has no right to process the data generated. In Israel too, the results of health monitoring could not lawfully be made available to employer.



In some countries the concept of employers being responsible for providing a healthy working environment is enshrined in health & safety law



As the clash between ever-smarter technology and evermore developed privacy concerns intensifies, employers are left charting the narrow course between serving their own legitimate interests in monitoring and respecting their employees' privacy. Our research shows that although there are some pretty well-established general legal principles across the world, there are also plenty of pitfalls for the unwary to fall into. Therefore, it is crucial for employers to be aware of the ground rules at local level and to implement robust and proportionate policies.

# CONTACTS

#### AUSTRIA

#### Birgit Vogt-Majarek

birgit.vogt-majarek@sms.law

#### ARGENTINA

#### Rodrigo Funes de Rioja

rfr@funes.com.ar

#### Eduardo Viñales

eiv@funes.com.ar

#### BELARUS

#### Darya Zhuk

darya.zhuk@cobalt.legal

#### BELGIUM

### Chris Engels

chris.engels@claeysengels.be

#### Sophie Maes

sophie.maes@claeysengels.be

#### BRAZIL

#### Luiz Guilherme Migliora

luiz.migliora@veirano.com.br

#### José Carlos Wahle

jose.wahle@veirano.com.br

#### BULGARIA

#### Borislav Boyanov

b.boyanov@boyanov.com

#### Violeta Kirova

v kirova@bovanov.com

# CANADA

#### Grea McGinnis

gmcginnis@mathewsdinsdale.com

# David Defrancesco

dde frances co@mathews dins dale.com

# Keith Murray

kmurray@mathewsdinsdale.com

## CHILE

# Enrique Munita

emunita@munitaabogados.cl

### CHINA

# Zheng Xie

zxie@fangdalaw.com

# COLOMBIA

## Catalina Santos

csantos@bu.com.co

#### CROATIA

#### Saša Diviak

sasa.divjak@dtb.hr

#### CYPRUS

#### George Georgiou

george@gzg.com.cy

# CZECH REPUBLIC

#### Natasa Randlova randlova@randls.com

# DENMARK

# Morten Langer

mortenlanger@norrbomvinding.com

## Jørgen Vinding

jv@norrbomvinding.com

#### ESTONIA

#### Karina Paatsi

karina.paatsi@cobalt.legal

#### FINLAND

#### Seppo Havia

seppo.havia@dittmar.fi

#### Petteri Uoti

petteri.uoti@dittmar.fi

#### FRANCE

#### Pascal Lagoutte

lagoutte@capstan.fr

#### Jean-Michel Mir

mir@capstan.fr

#### GERMANY

#### Markus Bohnau

markus.bohnau@kliemt.de

#### GREECE

#### Konstantinos Kremalis

kkremalis@kremalis.gr

#### **Dimitrios Kremalis**

dkremalis@kremalis.gr

#### HUNGARY

#### Marianna Csabai

marianna.csabai@clvpartners.com

#### Nora Ovary-Papp

nora.ovary-papp@clvpartners.com

#### HONG KONG

#### Kathryn Weaver

kathryn.weaver@lewissilkin.com

#### ΙΝΝΙΔ

# Rohit Kochhar

rohit@kochhar.com

#### IRFLAND

#### Siobhra Rush

siobhra.rush@lewissilkin.com

#### Linda Hynes

linda.hynes@lewissilkin.com

#### Orly Gerbi

gerbi@hfn.co.il

#### Franco Toffoletto

sft@toffolettodeluca.it

# Kazutoshi Kakuvama

kazutoshi.kakuyama@amt-law.com

#### Κ Δ 7 Δ Κ Η S Τ Δ Ν

# Yulia Chumachenko

y.chumachenko@aequitas.kz

#### LATVIA

#### **Toms Sulmanis**

toms.sulmanis@cobalt.legal

#### LITHUANIA Žilvinas Kvietkus

zilvinas.kvietkus@cobalt.legal

#### LUXEMBOURG

#### **Guy Castegnaro**

guy.castegnaro@castegnaro.lu

#### Ariane Claverie

ariane.claverie@castegnaro.lu

#### MALTA

#### Matthew Brincat

mbrincat@ganadoadvocates.com

#### MEXICO

#### Jorge De Presno Arizpe

jorgedepresno@basham.com.mx

#### NETHERLANDS

### Henriëtte Bronsgeest

h.bronsgeest@bd-advocaten.nl

#### Erik Deur

e.deur@bd-advocaten.nl

#### NETHERLANDS - PENSIONS LAW

#### Roel Veugelers

roel.veugelers@bvza.nl

#### Onno F. Blom onno.blom@bvza.nl

# NEW ZEALAND

Peter Kiely kiely@ktc.co.nz

# NORWAY

#### Claude Lenth

cal@hjort.no

# PANAMA

#### Julio Cesar Contreras III jcontreras@anorco.com.pa

## José Miguel Navarrete

jnavarrete@anorco.com.pa

# PFRU

José Antonio Valdez joseantoniovaldez@esola.com.pe

# POLAND

Bartłomiej Raczkowski bartlomiej.raczkowski@raczkowski.eu

# PORTUGAL

# Inês Reis

ines.reis@pbbr.pt

# Bruno Soeiro Barbosa

bruno.barbosa@pbbr.pt

## ROMANIA

# Gabriela Dinu

gabriela.dinu@nndkp.ro

# Irina Anyukhina

ianyukhina@alrud.com

Milena Jakšić Papac

#### SERRIA

#### SINGAPORE **Desmond Wee**

desmond.wee@rajahtann.com

milena.papac@karanovicpartners.com

#### SLOVAKIA

#### Dušan Nitschneider

nitschneider@nitschneider.com

#### SLOVENIA

#### **Gregor Simoniti**

gregor.simoniti@selih.si

#### SOUTH KOREA

# Sang Wook Cho

swcho@yulchon.com

#### Iñigo Sagardov

#### is@sagardov.com

Román Gil rga@sagardoy.com

# SWEDEN

Jenny Hellberg jenny.hellberg@elmzell.se

# SWITZERLAND (GE)

# Alfred Blesi

alfred.blesi@blesi-papa.ch

#### roberta.papa@blesi-papa.ch

# SWITZERLAND (FR)

Roberta Papa

Jacques Schneider jacques.schneider@schneider-troillet.ch

anne.troillet@schneider-troillet.ch

# Anne Troillet

#### TURKEY

Erim Bener

#### erim.bener@bener.av.tr Maria Çelebi

#### maria.celebi@bener.av.tr UKRAINE

Oksana Voynarovska

# voynarovska@vkp.kiev.ua

# UNITED ARAB EMIRATES

#### Samir Kantaria s.kantaria@tamimi.com

#### UNITED KINGDOM Michael Burd

#### michael.burd@lewissilkin.com James Davies

#### james.davies@lewissilkin.com UNITED KINGDOM -

#### PENSIONS LAW Michaela Berry

michaela.berry@sackers.com Claire Carev

#### claire.carey@sackers.com Ferdinand Lovett

# UNITED STATES OF AMERICA

Jeff Mokotoff jmokotoff@fordharrison.com

ferdinand.lovett@sackers.com

# VENEZUELA

#### Victorino Márquez

vmarquez@dra.com.ve Alejandro Disilvestro adisilvestro@dra.com.ve

lus Laboris is a leading international employment law practice combining the world's leading employment, labour and pensions firms. With an unsurpassed geographic coverage of 55 countries, over 1400 lus Laboris lawyers help clients navigate the world of HR law every day.

Note that nothing in this publication should be treated as an authoritative statement of the law and it should not be relied upon without first taking legal advice.





www.iuslaboris.com

copyright Ius Laboris 2019

ISBN: 978-94-6380-333-5

