

## Ius Laboris Webinar

# Coronavirus and privacy: a clash of fundamental rights

Thursday 23 April 2020

12:00 — 12:45 (CEST)

»» 08/06/2020

# SPEAKERS

---



**Philip Nabben, Partner**  
Netherlands  
Bronsgeest Deur Advocaten



**José Miguel Mestre Vázquez,**  
**Senior Associate**  
Spain  
Sagardoy Abogados



**Marie Behle Pondji, Counsel**  
Luxembourg  
Castegnaro



**Alexander Milner-Smith, Partner**  
United Kingdom  
Lewis Silkin



## **Philip Nabben**

Partner

Bronsgest Deur Advocaten (Netherlands)

[p.nabben@bd-advocaten.nl](mailto:p.nabben@bd-advocaten.nl)

P: +31 20 30 53 336

# CORONAVIRUS AND PRIVACY

---

## ISSUES TO BE DISCUSSED:

1. Honouring privacy versus containing spread of coronavirus: legal dilemmas
2. European context
3. Working from home: privacy issues
4. The use of apps: privacy & ethical questions
5. Wrap up



# CORONAVIRUS AND PRIVACY

---

## LEGAL DILEMMAS

- Balancing act: safe workplace versus privacy of sick employees
- Under the GDPR consent is no legal ground for processing personal data
- In the corona-crisis, employers are facing new legal dilemmas, including:
  - Can we take people's temperatures on entry (both staff and non-staff)?
  - Can we (or must we) reveal the name of an employee infected with coronavirus to colleagues and/or third parties?
  - May we send a sick employee home? What remedies are available if they refuse?



# CORONAVIRUS AND PRIVACY

---

## NEW DEVELOPMENTS, NEW QUESTIONS

The possible use of a government-issued app raises new questions and unprecedented ethical discussions, including:

- As an employer, could you compel your staff to install an app?
- Could you deny people who refuse to do so access to the office and could you stop payment of salary?
- If the app alerts you that an employee must stay in quarantine for 2 weeks, are they still entitled to be paid?
- Are we sure these apps have been sufficiently tested in terms of their usefulness, necessity and effectiveness?
- How do we know for sure that all data collected by the apps will be deleted afterwards?



# CORONAVIRUS AND PRIVACY

---

## SCENARIO:

**A large multinational, XYZ Ltd., has come to us for advice on privacy rights in the time of coronavirus.**

They want to know how to protect the privacy of their staff whilst at the same time processing personal data to enable them to control the risks of the coronavirus and protect their business.

***Let's take a look at the questions this raises.***



## **José Miguel Mestre Vázquez**

Senior Associate

Sagardoy Abogados (Spain)

[jmv@sagardoy.com](mailto:jmv@sagardoy.com)

P: +34 93 48 72 003

# EUROPEAN CONTEXT ON EMPLOYEE HEALTH INFORMATION

**Recital 46 GDPR:** “processing of personal data to protect an interest essential for the life of the data subject or that of another natural person.”

**Article 6.1d):** legal base: “the **vital interests** of data subject or of another natural person.”

However **Article 9.1 prohibits** processing such special category of data.

**Exception: Article 9.2 b):** “to carry out obligations and exercising rights of the controller of the data subject” (i.e. the employer).

**Article 9.2h):** “necessary for preventive or occupational medicine, medical diagnosis, etc.”

**Article 15 ePrivacy Directive:** “Member States to introduce measures to safeguard public security: as necessary, appropriate and proportional” (ECJ and ECHR).



# EUROPEAN DATA PROTECTION BOARD

## STATEMENT, 19 MARCH 2020

- Data protection rules (such as the GDPR) do not hinder measures taken to fight coronavirus, including measures to curb the spread of the disease, such as modern techniques
- The GDPR allows public health authorities and employers to process personal data in the context of an epidemic
- Processing of personal data can be done if necessary to fulfil obligations relating to health and safety at the workplace
- There must be transparent information on processing, retention period and purposes
- Mobile location data should be anonymised. If not, local adequate and proportional safeguards must be taken.



# GUIDELINES FROM EUROPEAN PRIVACY WATCHDOGS

## VARIOUS APPROACHES BY DATA PROTECTION AUTHORITIES

Despite Article 60 of the GDPR and close cooperation:

- **Italy:** employers were told to ***refrain*** from widely and systematically collecting information
- **France (CNIL):** “employers ***could not adopt measures*** that might breach the privacy of individuals”
- **Germany (BFDI):** published an article ***allowing*** for the gathering of employee health information regarding infection by coronavirus.



# LUXEMBOURG – COUNTRY SPECIFICS

---

## PROHIBITED

- The systematic and large scale collection of personal data (e.g. symptoms, temperature, etc.)
- The use of medical questionnaires or statements of absence of coronavirus symptoms
- The disclosure of names and other private data relating to infected employees

## RECOMMENDED

- Raising of awareness, and training and empowering employees
- Providing dedicated channels to enable people to report coronavirus infection (or suspicion) in a privacy-compliant way
- Directing employees to public health authorities and occupational health services

**Note:** If the government imposes more restrictive measures, those measures will prevail



## NETHERLANDS – COUNTRY SPECIFICS

## THE DUTCH DPA IS STILL BEING SUPER STRICT

**...As these quotes from their website show:**

*“As an employer, you may **not** check your staff for coronavirus yourself.”*

*“Only a company doctor may monitor employees. The doctor may then only share the result with the employee.”*

*“You **cannot** ask your employees about their health or take a test to check.”*

*“You may not keep a record of the reason someone calls in sick.”*

*“Your employee does **not** have to tell you that he or she has coronavirus”*



# UNITED KINGDOM – COUNTRY SPECIFICS

---

## CONTINUATION OF UK'S NORMAL POSITION:

The UK Information Commissioner's Office (ICO) has been practical and reasonable in its guidance, which reflects a continuation of the UK's normal position re processing health data in relation to the health and safety of employees (i.e. more permitted than some other EU countries). Specifically:

- **Asking individuals about their health (or recent travel):** The ICO confirms it is reasonable for companies to ask people whether they have coronavirus symptoms or have visited a particular country, but this is still subject to the usual GDPR principles of proportionality, necessity, notice, limits on retention and security etc.
- **Disclosing names of affected individuals:** In the ICO's view, an employer may inform its staff that there has been a case (or suspected case) of coronavirus, in order to discharge its duty of care to protect the health of employees. Employers should, however, consider whether sharing the name of affected individuals is strictly required to protect the well-being of others.
- **Responding to rights requests:** Whilst it cannot amend statutory deadlines, the ICO has suggested it is unlikely to take action if organisations process requests more slowly than usual. It will use its communication channels to inform data subjects that they may experience delays when exercising their information rights.

# SPAIN – COUNTRY SPECIFICS

---

## EMPLOYERS MAY:

- Process health information and take necessary measures.
- Find out if any employee is infected and design a contingency plan. They may make **limited inquiries** about symptoms, diagnosis or quarantine.
- This information should be disseminated to the workforce without identifying the infected employee, unless the authorities indicate otherwise.

## EMPLOYERS MUST:

- Protect health and safety at the workplace and keep it free of health risks. This enables them to **request information** from employees and visitors about symptoms or risk factors without specific consent.
- Process such data, respecting the limited purpose of it and minimising the storage period.

## EMPLOYEES MUST:

- Inform the employer if they become infected, so that they can be confined. If they go on sick leave, the employer is entitled to know the reason is coronavirus.

**NOTE:** The DPA understands we are in an emergency, but stresses that the principles of necessity and proportionality must be adhered to and personal data cannot be collected indiscriminately.



## **Marie Behle Pondji**

Counsel

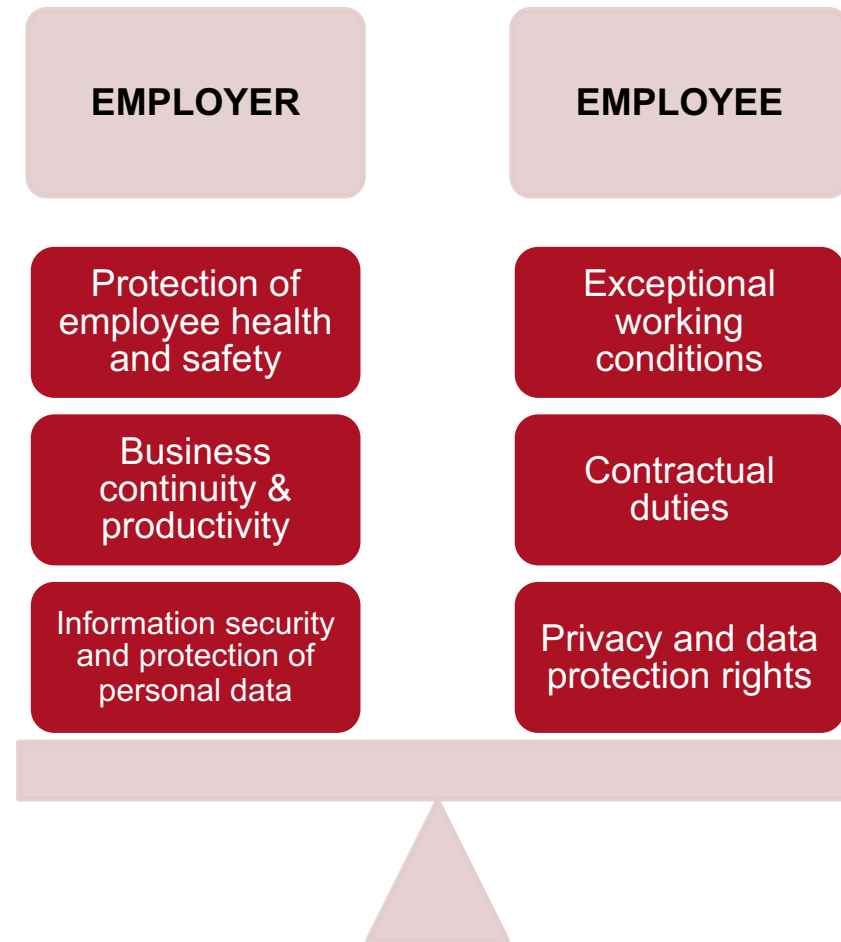
Castegnaro (Luxembourg)

[marie.behle@castegnaro.lu](mailto:marie.behle@castegnaro.lu)

P: +35 22 68 68 21

# WORKING FROM HOME – EUROPEAN PRIVACY ASPECTS

---



# WORKING FROM HOME – EUROPEAN PRIVACY ASPECTS

## SECURITY OF PERSONAL DATA:

- GDPR 'accountability' principle
- Vicarious liability

## RECOMMENDED BEST PRACTICE:

Take appropriate IT security measures (VPN, firewall, antivirus encryption, etc.)

Remind employees of existing IT / information security / data protection policies

Comply with industry security standards

Give employees:  
training  
guidance  
guidelines

Update contractual arrangements

# WORKING FROM HOME – EUROPEAN PRIVACY ASPECTS

## MONITORING EMPLOYEES' PRODUCTIVITY AT HOME?

- Right to respect for private life and correspondence (ECHR case law)
- GDPR requirements
- Respect for teleworker privacy (European Framework Agreement on Telework (2002))
- Additional requirements from Member State domestic law (e.g. in Luxembourg)

## RECOMMENDED BEST PRACTICE:

Rely on existing monitoring systems or internal regulations, if any

Involve the Data Protection Officer in the decision-making

Assess the need for a DPIA

Comply with local law

Update GDPR documentation

# SPAIN – COUNTRY SPECIFICS

The DPA has reported an increase in phishing, ransomware and other cyberattacks.

Note the obligation to communicate all security breaches to the authorities (Articles 33 and 34 GDPR).

## 1. Where the employer provides the resources:

- A policy must be implemented with technical and organisational measures to ensure compliance with health and safety rules
- All measures taken must preserve the confidentiality and integrity of personal data provided by employees.

## 2. Where the employer allows personal devices for telework:

- A VPN connection must be created to ensure security and remote access to databases.
- Firewalls, antivirus and proxy server obligations must be respected by employees when accessing databases and applications
- Employees must complete training in data protection, covering how to use programs, save information in the cloud, use eraser tools, etc.





# NETHERLANDS – COUNTRY SPECIFICS

---

## NO EXEMPTIONS FROM LEGAL DUTIES

### Working from home:

- No guidance from the AP, other than 4 tips for working from home (how to work in a safe environment, protect sensitive documents and use video chatlines with care)
- Generally, the pandemic does not exempt employers from their legal duties in relation to data security

### Employee monitoring:

- The coronavirus does not alter the restrictions on employee monitoring
- Advice: check your company's current policy on employee monitoring and follow it.

# UNITED KINGDOM – COUNTRY SPECIFICS

---

## TWO ASPECTS CLEARLY DEMARCATED:

- **Controller duties to protect data:**
  - Follow ICO very clear and simple guidance that: “organisations need to consider the ***same kinds of security measures*** for homeworking that you’d use in normal circumstances”
  - Follow National Cyber Security Centre guidance
  - Have a home working policy and information security policy
- **Controller duties to protect data subject workers (i.e. data rights and health and safety):**
  - Broadly the reverse – treat them ***in the same way*** as you would treat them at work
  - The ICO has been very clear that it does not want to see any compliance creep re monitoring because of the pandemic. Its message is that we need to be able to trust our employees and should avoid overly ‘creepy’ techniques particularly where more proportionate measures are available to monitor productivity

# LUXEMBOURG – COUNTRY SPECIFICS

---

## NO EXEMPTIONS FROM LEGAL DUTIES

- The pandemic does not exempt employers from their legal duties in relation to data security and does not eliminate restrictions on employee monitoring
- Monitoring systems cannot be installed without following the Labour Code procedure, which says:
  - written notice must be given to employees and the staff delegation (or Labour Inspection)
  - installation is not permitted until the DPA has had one month in which to offer its compliance assessment opinion
  - offending employers may face criminal prosecution



## **Alexander Milner-Smith**

Partner

Lewis Silkin (UK)

[alexander.milner-smith@lewissilkin.com](mailto:alexander.milner-smith@lewissilkin.com)

P: +44 (0)20 7074 8196

# CORONAVIRUS TRACING TECHNIQUES

---

## TRACING AND APPS

**1. Contact tracing techniques** seek to ascertain whether any individual has been in contact with an infected person during the time they were possibly infectious. Contact tracing could be used to support prompt communications with individuals who may be at risk of infection to ensure they:

- are aware of the risk;
- are provided with the appropriate information;
- take the appropriate steps to protect themselves and others; and
- receive any other support they may need.

**2.** There have been a number of reports about **Covid-19 tracing apps** over the last few weeks:

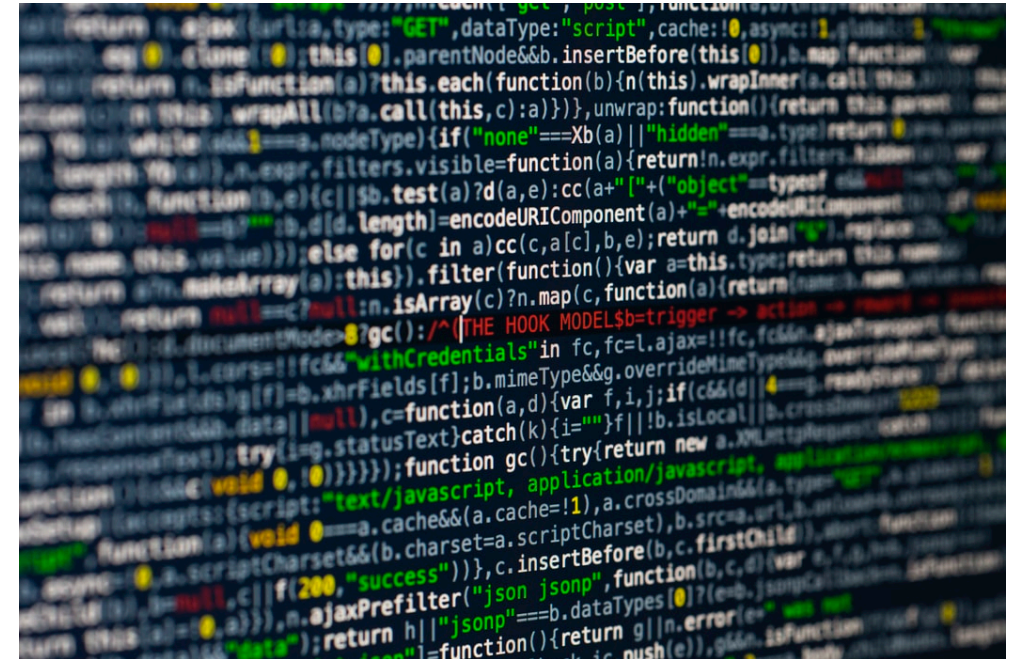
- Google and Apple LE Bluetooth will establish what the ICO is calling the Contact Tracing Framework, allowing links to be made between phones that have been in close proximity.
- It seems likely that governments will use this technology if and when they release their tracking apps. For example the UK government has confirmed it will release an app enabling people to self-report symptoms of the coronavirus. The app will then alert other people who have been in contact with them. It will very likely use the CTF.

# CORONAVIRUS TRACING APP

## DOES THE GDPR APPLY? - YES!

The European Data Protection Board comments:

*“The development of the apps should be made in an accountable way, documenting with a data protection impact assessment all the implemented privacy by design and privacy by default mechanisms...”*



# CORONAVIRUS TRACING APP

---

## **BUT, TO FOCUS ON EMPLOYER CONSIDERATIONS:**

- Can an employer force its personnel to install the app? CYOD (choose your own device) versus BYOD (bring your own device)?
- Is an employer entitled to know if and when an employee receives a notification?
- Can an employer deny access to the workplace if they refuse (either to install app or if they get a notification)? And if yes, can the employer, in that case, stop payment of salary?
- What if public transportation is not allowed without the app and the employee doesn't have the app and therefore can't come to work?
- Is the employee entitled to payment of salary if the app alerts that them to be in quarantine for 2 weeks?



# COUNTRY SPECIFICS

---

## SPAIN:

- The national government and certain regional ones have launched an app to track how the coronavirus evolves.
- It will help detect the disease, follow the treatment of patients and check the pandemic's evolution 'to support decision-making.

## LUXEMBOURG:

- Government reluctance to support the development of a Covid-19 tracing app at national-level
- Prime Minister has repeated Luxembourg's commitment to protect citizens' privacy and personal data
- A European app would be a better, more consistent and more efficient option

## NETHERLANDS:

- The Dutch government is choosing a partner to develop an app and this is being followed closely by the Dutch Parliament.
- Privacy experts are offering a list of recommendations: that it should be voluntary, temporary, for a strictly specified purpose, reliable, anonymised, safe, user friendly, etc.

## UK:

- The ICO has given a cautious green light to the CTF that Google and Apple are working on to enable governments to end current coronavirus lockdowns.
- The Information Commissioner has stated that the proposed CTF appears to be "aligned with the principles of data protection by design and by default."
- But she is concerned about compliance creep (e.g. reports that the NHS might be able to de-anonymise location data to identify individuals in the app it is designing)



# CORONAVIRUS AND PRIVACY

---

## WRAP UP

1. Despite the EU's attempt to standardise the rules, privacy rules in the various EU countries are still fragmented
2. Country by country approach
3. Working from home: generally, employers need to consider the same kinds of security measures for homeworking as would be used in normal circumstances
4. Introduction of an app still uncertain

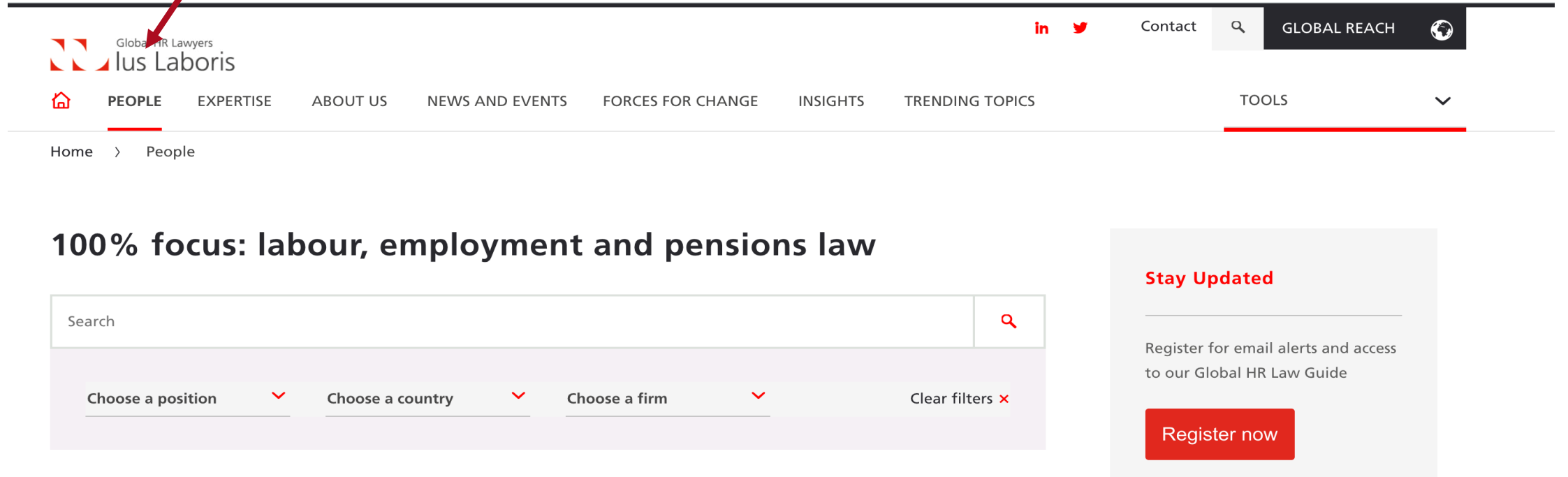
# QUESTIONS?

---



# IUS LABORIS – GLOBAL HR LAWYERS

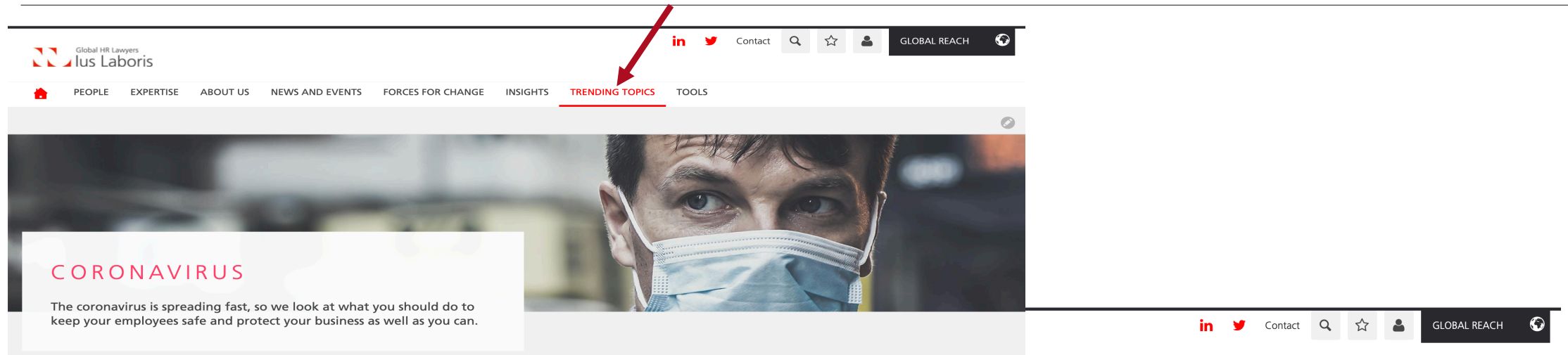
<https://www.iuslaboris.com/en-gb/lawyers/>



The screenshot displays the Ius Laboris website interface. At the top, the navigation bar includes the Ius Laboris logo (a red stylized 'IL' icon) and the text 'Global HR Lawyers Ius Laboris'. To the right of the logo are social media icons for LinkedIn and Twitter, a 'Contact' link, a search icon, and a 'GLOBAL REACH' button with a globe icon. Below the navigation bar is a horizontal menu with the following items: 'PEOPLE' (highlighted with a red underline), 'EXPERTISE', 'ABOUT US', 'NEWS AND EVENTS', 'FORCES FOR CHANGE', 'INSIGHTS', 'TRENDING TOPICS', 'TOOLS', and a dropdown arrow. Below the menu, a breadcrumb trail shows 'Home > People'. The main content area features the heading '100% focus: labour, employment and pensions law'. Below this is a search bar with the placeholder text 'Search' and a red search icon. Under the search bar is a filter section with three dropdown menus: 'Choose a position' (with a red dropdown arrow), 'Choose a country' (with a red dropdown arrow), and 'Choose a firm' (with a red dropdown arrow). To the right of these filters is a 'Clear filters' link with a red 'x' icon. On the right side of the page, there is a 'Stay Updated' section with a red heading. Below the heading is a text box that says 'Register for email alerts and access to our Global HR Law Guide'. At the bottom of this section is a red button with the text 'Register now'.

Questions and comments also welcome: [anni.laakso@iuslaboris.com](mailto:anni.laakso@iuslaboris.com)

<https://theword.iuslaboris.com/hrlaw/coronavirus>



## CORONAVIRUS: GUIDE FOR INTERNATIONAL EMPLOYERS

Sign up for our Guide for  
International Employers here:



Download the **Coronavirus: Guide for International Employers**.  
Or sign up to receive the guide and future updates in your inbox.

☐ Send me regular updates on international employment law news and trends.

**SIGN UP**

Last update: 06/04/2020



**North America:** Canada - Mexico - United States

**Central & South America:** Argentina - Brazil - Chile - Colombia - Panama - Peru - Venezuela

**Western Europe:** Austria - Belgium - Cyprus - Denmark - Finland - France - Germany - Greece - Ireland - Italy  
Luxembourg - Malta - Netherlands - Norway - Portugal - Spain - Sweden - Switzerland - United Kingdom

**Eastern Europe:** Belarus - Bulgaria - Croatia - Czech Republic - Estonia - Hungary - Latvia - Lithuania - Poland - Romania - Russia - Serbia - Slovakia - Slovenia -  
Turkey - Ukraine

**Middle East & Asia Pacific:** Bahrain - China - Hong Kong - India - Israel - Japan - Kazakhstan - New Zealand - Saudi Arabia - Singapore - South Korea -  
Thailand - United Arab Emirates

[www.iuslaboris.com](http://www.iuslaboris.com)