

In this week's issue:

- **Remote working:** To be or not to be?
- **Defining Work:** Continuing questions around work and working time.
- **EU:** Parliament adopts “due diligence” report
- **EU:** Vaccine passport proposals
- **Covid-19:** UK managers back mandatory vaccine for returning staff
- **Data Transfers:** The UK’s “data dilemma”
- **EU:** Gender pay transparency
- **Cyber-Security:** Data privacy and WFH IT security on a collision course?
- **BEERG Bytes:** New BEERG Byte on fake news – available also as a Podcast

Remote working: To be or not to be?

In an [article](#) for the *Guardian*, Professor Nicholas Bloom, professor of economics at Stanford University, specialising in management practices and uncertainty, writes:

“As companies come to decisions on new working arrangements, they will be essentially making a basic trade-off: the expectation of greater creativity in new projects at the office, but greater productivity on existing tasks at home. And, as with most trade-offs, the right answer is not all or nothing – five days or zero days at home – but something in the middle. It seems, from talking to more than 100 firms, this would be three days a week in the office.”



Professor Bloom goes on to say:

In the coming months and years, the radical shift towards working from home that occurred during the pandemic is setting up society for a new reality. For many of us, the Monday to Friday 9 to 5 daily commute will end. Instead, we will be working from home two days a week and travelling in to the office three days a week (or a formulation close to that), many of us from the suburbs and beyond. Ultimately, if this shift goes well, we have the potential to be more productive in our jobs and happier with a more balanced working life.

But he cautions that remote working will not be possible for everyone and that management needs to be careful about creating new divisions in the workforce between those who can work remotely and those who must turn up every day.

However, according to a new survey from KPMG ([here](#)) the “CEOs of the world’s most influential companies are planning what a return to ‘normal’ will look like, but their workforces’ lack of access to a

COVID-19 vaccine is forcing them to rethink their strategies”. With only one-third (31%) anticipating a return to normal in 2021, nearly half (45%) expect normality to resume in 2022. Significantly, 24% of leaders say that their business has changed forever.

Just 17% say they will downsize their company’s physical footprint, whereas 69% of those surveyed in August 2020 said they would do so. And just 30% will have a majority of employees working remotely between 2-3 days per week.

See also this interview with the CEO of Manpower, Jonas Prising, in *City A.M.* in which he [says remote working “isn’t unsustainable” but “it’s certainly undesirable.”](#) And that a move to a fully remote working culture will be very small indeed.

Defining Work: Continuing questions around work and working time.



Some weeks back, the UK Supreme Court in its *Uber* decision held that Uber drivers should be regarded as working from the time they logged onto the Uber App, though Uber has since said that it will only give drivers pay and benefits, such as holiday pay, when they actually have a passenger in their car. Whether Uber can decide which parts of a Supreme Court judgement to apply and which parts to ignore remains to be seen.

Last week, in another [judgement](#) touching on working time, the Supreme Court decided that workers in care homes who were obliged to sleep in overnight were not working while they were sleeping and could only be regarded as working when they actually had to get up during the night and attend to patients. (*For a detailed comment on this judgement see [here](#)*). It is worth noting that the Uber drivers are mostly men, while the care home workers are mostly women.

In recent weeks the Court of Justice of the European Union (CJEU) has ruled that a worker on “stand-by” at home is to be considered working if certain conditions are met (*see last week’s newsletter*).

As Sarah O’Connor [notes](#) in the *Financial Times*, about the two UK Supreme Court decisions:

“The cases don’t just matter for the parties involved. Taken together, they show the law is incoherent and under-enforced on a matter of growing importance: how we define “work” and ensure people are paid fairly for it, even as the boundaries of the workplace and the working day are beginning to dissolve.”

Colin Leckey and colleagues from Lewis Silkin say in a comprehensive [survey](#) of global development around the definition of work:

Questions of employment status continue to preoccupy courts and legislators, as new technology and new ways of working pose a challenge to traditional definitions of employee and contractor. Cases on this issue are being brought around the world, many of which revolve around taxi and delivery drivers engaged through digital platforms.

As businesses worldwide rethink post-Covid employment models, increasingly, as we pointed out in the recently-published HR Policy/BEERG discussion paper, *Beyond Taxis and Take-outs*, the questions that will be asked include:

- *What are you working on?*
- *Who are you working for?*

- Why are you doing this work?
- Where are you doing the work?
- When are you at work and when are you working? (When are you “on the clock”?)
- How do you do your work?

This debate is only beginning.

EU: Parliament adopts “due diligence” report



On 10 March, the European Parliament adopted a legislative initiative ([here](#)), calling for an EU directive on Mandatory Human Rights, Environmental and Good Governance Due Diligence for companies operating in the EU. The initiative is designed to put pressure on the European Commission to table such an initiative and to shape its content.

Such parliamentary initiatives are not binding on the Commission but can be indicative of the direction of travel and a signpost to where things might end up.

MEPs say:

"The exercise of due diligence requires undertakings to identify, assess, prevent, cease, mitigate, monitor, communicate, account for, address and remediate the potential and/or actual adverse impacts on human rights, the environment and good governance that their own activities and those of their value chains and business relationships may pose."

The due diligence obligation requires companies to get to know their supply chains in detail and understand the risks that may be posed to:

- **human rights**, including rights recognised in the Charter of Fundamental Rights of the European Union human rights and various other charters and conventions related to social rights, trade union activities and investment chains;
- **the environment**, such as the impact on climate change, deforestation, water quality, the sustainable use of natural resources, biodiversity and ecosystems; and
- **good governance**, including corruption, bribery, illegal campaign contributions and non-compliance with local tax legislation.

The Parliament proposes a wide definition of value chains catching all business and investment activities including direct and indirect business relationships upstream and downstream.

The obligation would apply to all large companies operating in the EU. This includes private or state-owned companies operating under the law of a Member State, established in the EU or operating in the internal market. Further, the obligation would apply to publicly listed or "high-risk" Small and Medium-sized Enterprises ("SMEs") and companies providing financial services and products.

A national authority would be responsible for supervising and enforcing the rules. In addition, the Parliament Initiative envisages a regime which would include fines ("**comparable in magnitude to fines currently provided for in competition law and data protection law**"), and temporary or indefinite exclusion

from public procurement, State aid and public support schemes, including schemes relying on Export Credit Agencies and loans.

The Commission is expected to present detailed legislative proposals during the coming months. For a detailed note on the Parliament initiative, see [here](#) from the law firm, White & Case.

EU: Vaccine passport proposals



More details have emerged of the European Commission's vaccine passport proposals.

"The certificate will make sure that the results shown are mutually recognised in every member state," the commission president Ursula von der Leyen said, adding that this digital or paper document will help reinstate freedom of movement in a "safe, responsible and trusted" way.

The EU's Digital Green Certificate will provide proof of Covid-19 vaccination, recovery or test results (both PCR test or rapid antigen test). They will be free of charge and available in digital form or on paper, both with a QR code and a digital signature to enable authentication.

National authorities such as hospitals and test centres will be responsible for issuing these documents. The documents will include the holder's name, date of birth, the issuing member state, and a unique identifier.

Depending on the certificate, other specific data will be displayed, such as the type of vaccine or test used, the date of vaccination, the test result, or the number of vaccines doses. And the proof of recovery will have to indicate the date of the positive test result, the issuer and the date of issuance.

This specific document should be issued at the earliest from the 11th day after the first positive test and should be valid for not more than 180 days, the commission said.

EU countries should issue vaccination certificates for people who have received any of the jobs approved by the European Medicine Agency, but they can decide to accept other vaccines that have only been approved in a specific member state.

So far, BioNTech/Pfizer, Moderna, AstraZeneca, and Johnson & Johnson vaccines are the only jobs approved in the EU.

Covid-19: UK managers back mandatory vaccine for returning staff



More than half of managers in the UK want to be allowed to make coronavirus vaccinations mandatory for staff returning to work, according to a survey of 1,000 managers from the Chartered Management Institute. Close to half said office access should be restricted for those who refused to get a vaccination on non-medical grounds.

Three-fifths of managers have already decided to make testing available for staff when they are allowed to return — with a fifth saying this will become mandatory to return to work.

However, lawyers warn that it would be difficult for companies to insist on mandatory vaccinations under current workplace legislation, given the risk of discriminating against workers who cannot or will not be vaccinated.

Meanwhile in Israel, a court has upheld a school's decision to bar a teaching assistant who had refused to show proof she had been vaccinated or tested for COVID-19. A court spokeswoman said she believed it was Israel's first ruling on COVID-19 policy in the workplace, though it could still be overturned on appeal. Some Israeli schools, in reopening, have required that their staff show proof either of vaccination or negative once-weekly COVID-19 tests.

The teaching assistant refused to give proof of either, citing her right to privacy and freedom of conscience. Banned from school in response, she took legal action, arguing she had suffered de-facto suspension. She argued that the school's policy was an unlawful breach of her medical privacy and that she was being pressured to get vaccinated against her beliefs.

"We do not, at this time, believe that the apparent rights of the appellant outweigh the right and duty of the respondent to care for the welfare of their pupils, educational staff and pupils' parents," the court said.

Data Transfers: The UK's "data dilemma"



On March 19, 2021, the UK Secretary of State for Digital, Culture, Media & Sport ("DCMS") signed a [Memorandum of Understanding](#) ("MoU") with the UK Information Commissioner's Office (the "ICO") with respect to new UK adequacy assessments following the UK's departure from the European Union. The MoU sets out how DCMS and third countries will negotiate adequacy decisions, referred to under the MoU as "adequacy regulations". These "regulations" will permit the free transfer of personal data collected in the UK to the relevant "adequate" jurisdiction.

For the moment, the UK has adopted the existing adequacy decisions of the European Commission prior to Brexit but will in the future make its own adequacy decisions. Although these decisions will be the responsibility of the Secretary of State, the Secretary must consult the ICO (and other persons they consider to be appropriate) prior to making any such decision. DCMS and the ICO are required by the MoU to work closely together, sharing expertise and information, but ultimately DCMS is not bound in its decisions by the views of the ICO.

The MoU sets out the four phases through which DCMS will conduct its adequacy work, commencing with "gatekeeping", the process by which a specific team within DCMS will consider whether to commence an assessment of a third country for adequacy purposes. This phase is followed by an assessment (based on the requirements of Article 45 of the GDPR), a recommendation to the Secretary of State and finally a procedural phase, during which the adequacy regulations will be drafted and laid before parliament. The ICO and DCMS are expected to meet for discussion at various intervals during this process.

The UK government stated after signing the MoU that it "intends to expand the list of adequate destinations in line with our global ambitions and commitment to high standards of data protection."

However, as we noted in our recent Brexit Briefing ([here](#)) none of this provides an answer to the UK's "data dilemma". If the UK grants adequacy decisions to jurisdictions that do not have an EU adequacy decision, then will the EU continue to allow personal information to flow from the EU to the UK in the knowledge that it could be forwarded to third countries? Assuming, of course, that the EU grants the UK an adequacy decision in the first place.

In a way, this is similar to the UK's food standards dilemma. Does the UK agree to continue to follow EU food standards to ease UK exports to the EU ([here](#)) or does it refuse to do so to facilitate a trade deal with the US whose food standards differ from those of the EU?

A UK/US trade deal may be some way down the road given the priorities of the Biden administration, so the food standards choice may not become an issue anytime soon.

The "data dilemma", however, will present itself as soon as the UK gives an adequacy decision to a third country with which the EU does not have an adequacy arrangement. The dilemma will become even more acute if the first country chosen happens to be the US.

EU: Gender pay transparency



On 4 March 2021, the European Commission presented a proposal on pay transparency which aims to ensure that women and men in the EU receive equal pay for equal work. The legislative proposal focuses on two core elements of equal pay (i) measures to ensure pay transparency for workers and employers; and (ii) access to justice for those experiencing pay discrimination.

Pay transparency measures:

- **Pay transparency for job-seekers** – Employers will have to provide information about the initial pay level, or its range in the job vacancy notice, or before the job interview. Employers will not be allowed to ask prospective workers about their pay history.
- **Right to information for employees** – Workers will have the right to request information from their employer on their individual pay level and on the average pay levels, broken down by sex, for categories of workers doing the same work or work of equal value.
- **Reporting on gender pay gap** – Employers with at least 250 employees must publish information on the pay gap between female and male workers in their organisation. For internal purposes, they should also provide information on the pay gap between female and male employees by categories of workers doing the same work or work of equal value.
- **Joint pay assessment** – Where pay reporting reveals a gender pay gap of at least 5 % and when the employer cannot justify the gap on objective gender-neutral factors, employers will have to carry out a pay assessment, in cooperation with workers' representatives.

Access to justice:

- **Compensation for workers** – workers who suffered gender pay discrimination can get compensation, including full recovery of back pay and related bonuses or payments in kind.
- **Burden of proof on employer** – it will be by default for the employer, not the worker, to prove that there was no discrimination in relation to pay.
- **Sanctions to include fines** – Member States should establish specific penalties for infringements of the equal pay rule, including a minimum level of fines
- **Equality bodies and workers' representatives** may act in legal or administrative proceedings on behalf of workers as well as lead on collective claims on equal pay.

It now falls to the Council of Ministers and to the European Parliament to consider the Commission's legislative proposals. Given the usual legislative timetable, it could be several years before any new law becomes operative at national level.

CyberSecurity: Data privacy and WFH IT security on a collision course?



[Derek Mooney](#) writes: Over the past 12 months we have become all too familiar with reading depressing and worrying statistical trends, such as increasing R numbers, daily new infection rates and, sadly, mortality figures. While steadily increasing vaccination rates (depending on where you are based) are now forcing these Covid-19 numbers down, there is another set of numbers, more indirectly related to Covid19 which seem to be still going up: the number of cyber security incidents.

The security company PurpleSec reckons that cybercrime has increased by up to 600% in 2020 alone. They attribute a large part of this growth to the new opportunities presented by the existence of many more remote work environments due to the Covid-19 pandemic, particularly ransomware and phishing attacks.

PurpleSec's [2021 Trends Report](#) highlights the threat it sees from a range of attacks on those working from home, including so-called *Drive-By Wireless Attacks* which opportunistically impact remote workers where they are living. The equipment to do it is cheap and the net is full of how-to-hack videos. PurpleSec quotes a Microsoft Digital Defence Report that says that the volume of IoT attacks in the first half of 2020 rose by 35% compared to the second half of 2019.

The real difficulty comes, however, as this very comprehensive [DLA Piper blog](#) highlights as network monitoring, one of key security tools designed to prevent, detect and manage cyberattacks — can involve continuous surveillance and processing of employee personal information and thus sets IT security and data privacy rights on a collision course. The Blog, which takes a look at varying requirements across the globe, strongly urges employers, particularly multinational ones, to fully consider the data privacy and employee network monitoring laws in all jurisdictions when trying to mitigate WFH cyber risk. The Blog concludes:

Perhaps the most critical takeaway on network monitoring is the necessity of planning ahead. Too often companies are implementing new or enhanced monitoring tools in the aftermath of a harmful breach of their systems that have led to significant financial or reputational loss, as well as the prospect of litigation and enforcement. The urgency of standing up improved techniques against cyber-attacks may come at the cost of thoughtful consideration and implementation of the varied obligations imposed by data protection and other laws.

DLA Piper Blog by [Carol A.F. Umhoefer](#) and [Alaa Salaheldin](#) can be found here: blogs.dlapiper.com

BEERG Bytes: New BEERG Byte on fake news – also available as a Podcast



Our latest BEERG Byte looks at the issue of digital hate and fake news and features Imran Ahmed CEO of the London and Washington DC based, [Center for Countering Digital Hate](#). Don't forget that all our BEERG Bytes from 2021, along with many from 2020, are all available as Podcasts – search for "BEERG Bytes" via your favourite [Podcast](#) search engine such as Spotify or Google or using the links below. You

can view current and archived episodes as videocasts, online at www.beerg.com/beergbytes

BEERG Bytes on: [Spotify](#) / [Google Podcasts](#) / [Apple Podcasts](#) / [Anchor RSS](#)

BEERG Events in 2021:

BEERG meetings and events will remain online only up to September 2021.

We will revisit this position after June 2021 in the light of the vaccination programme roll-out across Europe and the US, and official travel advice.

TBC BEERG 2021 Dates for your Diary:

Date	Event	Venue
TBA	BEERG Members' Network Meeting [Oct]	TBC
TBA	BEERG Training Programme [Oct]	TBC