Eurostat monitoring report – How has the EU progressed towards the Sustainable Development Goals?

Sustainable development aims to achieve a continuous improvement in citizens' quality of life and well-being, without compromising the well-being of future generations. This involves the pursuit of economic progress, while safeguarding the natural environment and promoting social justice. For these reasons, sustainable development is a fundamental and overarching objective of the European Union and the progress towards the goals agreed at UN level is regularly monitored and reported.

Full text available on EUROSTAT website

Remarks by President Juncker at the joint press conference with President Tusk ahead of the G20 Summit

Good morning,

Guten Morgen,

Buongiorno,

Bom Dia,

There is no better place for this year's G20 Summit than here in Osaka – a vibrant merchant city, known as the 'Nation's Kitchen'.

As we prepare to discuss the future of the global economy over the next two days, we should inspire ourselves by the city's rich history of innovation and openness.

We meet at a time when the global economy continues to grow despite some clouds forming on the horizon.

Amongst this uncertainty, Europe's economy continues its stable and sustainable growth. We are now in the seventh consecutive year of economic growth, on average 2%, with every Member State contributing to that progress.

Investment is finally back to the pre-crisis level. Unemployment is at a record low since the turn of the century and more people are in work than

ever before, 240.7 million to be exact. 13.4 million of those jobs have been created since November 2014.

A large part of this success is due to the fact that Europe is open for fair business. The European Union is the number one trading partner for 80 countries around the world. We have 72 trade agreements in place, and under the mandate of this Commission alone we have opened up trade relations with 15 countries – from Canada to Japan via Ukraine and Ecuador.

And there is more good news to come. This Sunday, the Commission will sign the new EU-Vietnam trade and investment agreements.

This will not only take our trade relation to the next level, but it will also help strengthen respect for human, environmental and workers' rights. This is what Europe's trade policy is about.

We believe in trade, because it works for us and for others. 36 million jobs in the European Union are supported by exports and almost 700,000 small businesses benefit from international trade.

But we are not naïve free traders. In the last five years, we have adopted 42 new anti-dumping and anti-subsidy measures. And we have introduced an investment screening mechanism and I hope that the Commission's proposal for an Investment Procurement Instrument will also be adopted swiftly.

This shows that we will stand up for ourselves if others do not play by the rules. But it also reveals the loopholes in the global trading system which have created the trade tensions we see across the world. We have to tackle this issue head on.

In this spirit, I believe that the Global Forum on Steel Excess Capacity should have its mandate extended so that it can deliver on existing commitments.

We are also working closely with the United States and Japan, as well as China and others, on reforming the World Trade Organization and creating a level playing field. We must tackle issues such as unfair industrial subsidies and the forced transfer of technology. This can only be done with the G20 as a core group driving this forward.

This is about ensuring that the rules of the game are fit for the modern, digital economy. This is why the European Union also fully supports Prime Minister Abe's Data Free Flow with Trust initiative to facilitate the cross border flow of data among countries with high levels of privacy protection.

This cooperative approach also sums up Europe's attitude to the G20 and to the multilateral rules-based system as a whole.

And nowhere is this more important than when it comes to climate change. Europe will continue to lead the way, as we did in Paris in 2015. We have ambitious 2030 goals for renewable and energy efficiency which we must focus on implementing. We will do this by making sustainable financing a central part of our financial system, through the Capital Markets Union. And we will

invest 25% of the next long-term European budget in climate action.

But climate change will not stop in 2030 and there is a strong and significant majority of Member States of the Union that support the Commission’s climate neutral strategy for 2050. I believe it is the way forward – it is good for the planet and it is good for business.

On all of these issues, Europe is ready to lead at home and work with our G20 partners to offer stability and confidence the world needs.

We share many of the same challenges and we are undergoing many of the same transitions. Whether it be climate, digital or technological change, the issues that we will discuss over the next few days cut across boundaries, societies and economies. They require a concerted and comprehensive response within the multilateral rules-based system.

Our message to the world is clear and simple: Europe is committed to upholding – and where necessary updating – the rules-based global system. And we are ready to work with everyone to make that happen.

Thank you.

Sabine Lautenschläger: Euro Cyber Resilience Board for pan-European Financial Infrastructures

Introductory remarks by Sabine Lautenschläger, Member of the Executive Board of the ECB, at the third meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt am Main, 28 June 2019

It is a pleasure to welcome you back to Frankfurt. As you may know, I recently became responsible for market infrastructures and payments at the ECB. As this includes the ECB's work on the cyber resilience of financial market infrastructures (FMIs), I have taken over Benoît Cœuré's chairmanship of the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB). I would first like to thank Benoît for his contribution in establishing the ECRB and for this opportunity to continue the excellent work on cyber resilience at European level which he has personally driven forward.

Six months have passed since our last meeting in December, during which time, all of us – whether on behalf of a public or private financial infrastructure, a supervisor or an overseer – have been busy enhancing the cyber resilience of our respective financial infrastructures and of the financial sector as a whole. But cybercriminals have been making progress too, and they remain persistent and relentless in their pursuits. As widely reported in the press, a major cyber incident occurred at a significant bank earlier this year, seriously affecting the real economy in a specific European country. This publicly known incident reminds us of the debilitating impact a cyberattack can have on our financial system. So the need for continued vigilance, work and collaboration in this field is imperative.

You will recall that – in December 2018 – the ECB published its cyber resilience oversight expectations[1], a tool meant for both FMIs and overseers. These expectations contain detailed best practices for implementing the CPMI-IOSCO Cyber Guidance[2] and are now being followed by FMI operators at national and European level. Overseers are working with their respective FMIs to ensure that they do what is necessary to enhance their cyber resilience. I am also pleased that the World Bank has recently embraced our cyber resilience oversight expectations with a view to boosting the cyber resilience of FMIs in developing and emerging countries under its mandate, and consequently promoting global harmonisation.

Last year, the Eurosystem also developed the European Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU)[3]. Red teaming helps entities assess, by means of controlled "ethical hacking", if and how they are capable of withstanding a cyberattack. And because TIBER-EU involves high-end testing on live production systems, we are currently reflecting on how to foster an accreditation and certification capability in the EU. This would allow cybersecurity service providers to raise standards around threat intelligence and red team testing and to have their capabilities in this field validated.

I am pleased to say that, since its publication, TIBER-EU has been

implemented – or is currently being implemented – in Belgium, Denmark, Germany, Ireland, the Netherlands, Romania and Sweden, and by the ECB in its oversight capacity. The ECB is also in close dialogue with other EU and non-EU jurisdictions that are considering TIBER-EU as a tool for their respective financial sectors. The gradual roll-out of TIBER-EU will ensure that threat-led penetration testing is conducted in a harmonised way across the EU, avoiding duplication of work for financial entities and authorities alike.

Already in March 2018, at the first ECRB meeting, we presented the results of a cyber resilience survey that had been developed under the Eurosystem oversight cyber resilience strategy. The survey had been conducted across more than 75 payment systems, central securities depositories and central counterparties throughout Europe. You will recall that the survey highlighted a number of weaknesses prevailing at the time, such as cyber governance, training and awareness, and cyber incident response. Today we will update you on the second round of the cyber resilience survey, which we conducted again across mostly the same population of FMIs throughout Europe. The results have given us an insight into how the sector has progressed, and indeed, while we see improvement in some areas, there is still much to be done.

When we established the ECRB, the aim was essentially to create a forum for strategic discussions at board level, to raise awareness of the topic of cyber resilience, to catalyse joint initiatives to develop effective solutions for the market and to share best practices and foster trust and collaboration. In this context, I am very pleased that the spirit of the ECRB is living up to expectations. As you will recall from the UNITAS crisis communication exercise last year[4], we identified two key areas in which the ECRB could drive improvements forward: *information sharing* and *crisis management*. This year, thanks to your commitment and contribution, we have set up two working groups of experts drawn from your institutions and we have made significant progress in these areas. I would like to sincerely thank you for your contributions and for sustaining our spirit of trust and collaboration.

The ECRB working group on information sharing will tell us about their proposed model, which sets out the building blocks for sharing information and intelligence. It is clear that, among other things, financial infrastructures should have effective cyber threat intelligence processes; they should actively participate in information-sharing arrangements and collaborate with trusted stakeholders within the industry. The working group’s proposal seeks to address this by facilitating information and intelligence sharing, enabling you to better protect yourselves and the wider ecosystem. As discussed at our last meeting, regulatory reporting on cyber incidents is intentionally not part of this work.

We will also receive an update on the work of the ECRB working group on crisis management, and we will touch upon third-party risk and ecosystem recovery and coordinated reconciliation.

As you may guess from my brief remarks today, we have a great deal of work ahead of us. I believe that sharing information, knowledge and expertise among financial infrastructures and authorities in a non-regulatory context

remains essential for tackling the cyber challenge we all face. I am convinced that we can only do this by joining forces. I want to thank you for being here today and I look forward to a fruitful discussion.

EASO and Malta sign Operational and Technical Assistance Plan

The European Asylum Support Office (EASO) and the Maltese authorities have signed an Operating Plan for the deployment of Asylum Support Teams and the provision of technical and operational assistance to Malta up until 31 December 2019. The official document was signed by the Executive Director of EASO, Ms. Nina Gregori, and the Permanent Secretary of the Ministry for Home Affairs and National Security, Mr. Kevin Mahoney, on behalf of Malta.

At the request of the Maltese authorities, the Operational and Technical Assistance Plan Support (Operating Plan) will see EASO provide tailor-made assistance, including by providing capacity building and backlog management support, technical expertise and quality control tools.

The Operating Plan is intended to ensure that persons in need of international protection in Malta have access to the international protection determination procedure, and, specifically, that the procedure at first instance is concluded as swiftly as possible.

Commenting on the signature of the Operating Plan, **Ms. Nina Gregori** stated: *"EASO's core mandate is to support EU Member States in implementing the Common European Asylum System, including by rapidly deploying experts to provide assistance on-the-ground. Once again, we are delighted to be able to quickly and effectively provide tangible solidarity to a frontline Member State which has repeatedly proven to be an example of European solidarity itself."*

Through its support, EASO aims to help alleviate the pressure on the Maltese asylum system. The activities under the Operating Plan will be closely coordinated with the Maltese authorities, in consultation with the European Commission, and in complementary continuation of the fruitful cooperation with the UNHCR.

The 2019 Operational and Technical Assistance Plan agreed to by EASO and Malta can be consulted here.

Any further information may be obtained from the European Asylum Support Office on the following email address: press@easo.europa.eu.

Photo: © Getty Images/Oleksii Liskonih

Mergers: Commission approves acquisition of Red Hat by IBM

The European Commission has approved unconditionally, under the EU Merger Regulation, the proposed acquisition of Red Hat by IBM, both information technology companies based in the US. The Commission concluded that the transaction would raise no competition concerns.

Red Hat and IBM both sell information technology ("IT") solutions to enterprise customers. Red Hat's main activities relate to open-source software and support services, while IBM is active in a wide variety of IT solutions, namely enterprise IT software, hardware and services.

The Commission's investigation

During its investigation, the Commission assessed:

- The impact of the proposed transaction on the markets for **middleware and system infrastructure software**, where the activities of IBM and Red Hat overlap. Middleware is software used for making and operating enterprise application software, i.e. business-oriented tools, such as online payment processing. System infrastructure software allows companies to configure, control, automate and share the use of hardware resources (e.g. servers) across enterprise application software. The Commission found that the merged entity would **continue to face significant competition from other players** in all potential markets.
- Whether there would be a risk of weakened competition if IBM or Red Hat leveraged their respective positions into neighbouring markets. In particular, the Commission assessed whether IBM could significantly reduce the competitiveness of its rivals' offerings by degrading their interoperability with Red Hat's flagship product **Red Hat Enterprise Linux**. The Commission concluded that the merged entity would not have sufficient market power to shut out or marginalise its competitors by bundling or degrading interoperability. Moreover, as the success of Red Hat significantly hinges on its neutrality, any strategy impairing this neutrality would likely damage Red Hat's business, by shifting the focus of customers, developers and partners alike to competing open-source solutions.
- Whether the merged entity would be likely to degrade access to **Red Hat's source code** and/or influence the development of specific **open source projects** in order to ease (actual or potential) competition on its products. The Commission found that any such strategies would trigger strong adverse counter-reactions from the open source community of developers that would negatively affect Red Hat's products.

In addition, the Commission took note of the potential pro-competitive rationale of this acquisition. This reflects, in particular, IBM's intention

to use the complementary capabilities of Red Hat to further develop and offer open hybrid cloud solutions. This would increase choice for enterprise customers who could more easily shift workloads between on premise servers and multiple public and private clouds.

Therefore, the Commission concluded that the transaction would raise no competition concerns in any of the affected markets and cleared the case unconditionally.

Companies and products

IBM is a US based company active worldwide in the development, production, and marketing of a wide variety of IT solutions, namely enterprise IT software, IT hardware and ITservices.

Red Hat is a US based company active worldwide in the provision of open-source software and support services.

Merger control rules and procedures

The transaction was notified to the Commission on 20 May 2019.

The Commission has the duty to assess mergers and acquisitions involving companies with a turnover above certain thresholds (see Article 1 of the Merger Regulation) and to prevent concentrations that would significantly impede effective competition in the EEA or any substantial part of it. The vast majority of mergers do not pose competition problems and are cleared after a routine review.

From the moment a transaction is notified, the Commission generally has a total of 25 working days to decide whether to grant approval (Phase I) or to start an in-depth investigation (Phase II).

More information will be available on the Competition website, in the Commission's public case register under the case number M.9205.