EUROPEAN COMMISSION

MEMO

Brussels, 27 January 2014

Data Protection Day 2014: Full Speed on EU Data Protection Reform

Vice-President Viviane Reding, the EU's Justice Commissioner said ahead of data protection day (which is on 28 January): "*Data protection in the European Union is a fundamental right. Europe already has the highest level of data protection in the world. With the EU data protection reform which was proposed exactly two years ago – in January 2012 – Europe has the chance to make these rules a global gold standard. These rules will benefit citizens who want to be able to trust online services, and the small and medium sized businesses looking at a single market of more than 500 million consumers as an untapped opportunity. The European Parliament has led the way by voting overwhelmingly in favour of these rules. I wish to see full speed on data protection in 2014*."

Vice-President Reding will deliver a key speech on data protection day, tomorrow at 11 CET at the Centre for European Policy Studies (CEPS) **calling for "A new Data Protection Compact for Europe".**

1. Where are we two years after the Commission's proposals?

Two years ago, in January 2012, the European Commission proposed a reform of the EU's data protection rules to make them fit for the 21st century (see IP/12/46). The reform consists of a draft Regulation setting out a general EU framework for data protection and a draft Directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities. The proposals are currently being discussed by the two European Union co-legislators, the European Parliament and the Council of the EU in which national Ministers sit.

To become law, the proposals must be approved by these co-legislators.

European Parliament:

On 21 October 2013, the European Parliament's leading Committee on Civil Liberties, Justice and Home Affairs (LIBE) backed the Commission's proposals with an overwhelming majority and even reinforced them in certain areas (see MEMO/13/923 for full details). The reports of the members of the European Parliament (MEPs) Jan-Philipp Albrecht and Dimitrios Droutsas, on which members of the LIBE Committee voted, were welcomed as a strong endorsement of the Commission's package approach to the data protection reform, and an important signal of progress in the legislative procedure. The LIBE vote gives a mandate to its Rapporteurs, MEPs Albrecht and Droutsas, to enter into negotiations with the Council of the EU.

Council of the EU:

The data protection reform has been discussed repeatedly by national Ministers in the Justice Council. Most recently, Justice Ministers reached an agreement in principle on the "one-stop shop" mechanism (the proposal that every company operating in the single market should have a single regulatory interlocutor in the EU) at the Council in October 2013 (Council Press Release and SPEECH/13/788). The proposals were discussed again at the December Justice Council (see SPEECH/13/1029) and at the Informal JHA Council in Athens, on 23-24 January. An agreement on the reform is possible before the end of this year.

European Council

European heads of state and government committed to a "timely" adoption of the new data protection legislation at a summit on 24 and 25 October 2013, which focused on the digital economy, innovation and services (see Conclusions).

What are the next steps?

The data protection reform is a priority for the Greek Presidency. The Presidency convened a tripartite meeting in Athens (on 22 January) with the European Commission, the two European Parliament rapporteurs and the next Presidency of the EU (Italy) to work out a road map for agreeing on the data protection reform swiftly. The objective is to agree on a mandate for negotiation with the European Parliament before the end of the Greek Presidency.

The European Parliament is expected to adopt the proposals in first reading in the April 2014 Plenary session.

An agreement on the data protection reform is thus possible before the end of this year. As a comparison: the current 1995 data protection directive took five years to negotiate.

2. Which are the main benefits of the EU Data Protection Reform?

The European Commission proposals for a comprehensive reform of the EU's 1995 data protection Directive aim to strengthen privacy rights and boost Europe's digital economy. The Commission's proposals update and modernise the principles enshrined in the 1995 Directive, bringing them into the digital age and building on the high level of data protection which has been in place in Europe since 1995.

Benefits for citizens

There is a clear need to close the growing rift between individuals and the companies that process their data: nine out of ten Europeans (92%) say they are concerned about mobile apps collecting their data without their consent. Seven Europeans out of ten are concerned about the potential use that companies may make of the information disclosed (see Annex).

The data protection reform will strengthen citizens' rights and thereby help restore trust. Better data protection rules mean you can be more confident about how your personal data is treated, particularly online. The new rules will put citizens back in control of their data, notably through:

- **A right to be forgotten**: When you no longer want your data to be processed and there are no legitimate grounds for retaining it, the data will be deleted. This is about empowering individuals, not about erasing past events or restricting freedom of the press (see separate section on this).
- **Easier access to your own data**: A right to data portability will make it easier for you to transfer your personal data between service providers.
- **Allowing you to decide how your data is used**: When your consent is required to process your data, you must be asked to give it explicitly. It cannot be assumed. Saying nothing is not the same thing as saying yes. Businesses and organisations will also need to inform you without undue delay about data breaches that could adversely affect you.
- **The right to know when your data has been hacked**: for example, companies and organisations must notify the national supervisory authority of serious data breaches as soon as possible (if feasible within 24 hours) so that users can take appropriate measures.
- **Data protection first, not an afterthought**: 'Privacy by design' and 'privacy by default' will also become essential principles in EU data protection rules – this means that data protection safeguards should be built into products and services from the earliest stage of development, and that privacy-friendly default settings should be the norm – for example on social networks or mobile apps.

Benefits for business

Data is the currency of today's digital economy. Collected, analysed and moved across the globe, personal data has acquired enormous economic significance. According to some estimates, the value of European citizens' personal data has the potential to grow to nearly €1 trillion annually by 2020. **Strengthening Europe's high standards of data protection is a business opportunity.**

The European Commission's data protection reform will help the digital single market realise this potential, notably through four main innovations:

- **One continent, one law**: The Regulation will establish a single, pan-European law for data protection, replacing the current inconsistent patchwork of national laws. Companies will deal with one law, not 28. The benefits are estimated at €2.3 billion per year.
- **One-stop-shop**: The Regulation will establish a 'one-stop-shop' for businesses: companies will only have to deal with one single supervisory authority, not 28, making it simpler and cheaper for companies to do business in the EU; and easier, swifter and more efficient for citizens to get their personal data protected.
- **The same rules for all companies – regardless of their establishment**: Today European companies have to adhere to stricter standards than companies established outside the EU but also doing business on our Single Market. With the reform, companies based outside of Europe will have to apply the same rules. We are creating a level-playing field.
- **European regulators will be equipped with strong enforcement powers**: data protection authorities will be able to fine companies who do not comply with EU rules with up to 2% of their global annual turnover. The European Parliament has even proposed to raise the possible sanctions to 5%. Privacy-friendly European companies will have a competitive advantage on a global scale at a time when the issue is becoming increasingly sensitive.

Benefits for SMEs

The data protection reform is geared towards stimulating economic growth by cutting costs and red tape for European business, especially for small and medium enterprises (SMEs). First, by having one rule instead of 28 the EU's data protection reform will help SMEs break into new markets. Second, the Commission has proposed to exempt SMEs from several provisions of the Data Protection Regulation – whereas today's 1995 Data Protection Directive applies to all European companies, regardless of their size. Under the new rules, SMEs will benefit from four reductions in red tape:

- **Data Protection Officers**: SMEs are exempt from the obligation to appoint a data protection officer insofar as data processing is not their core business activity.
- **No more notifications**: Notifications to supervisory authorities are a formality and red tape that represents a cost for business of 130 million euro every year. The reform will scrap these entirely.
- **Every penny counts**: Where requests to access data are excessive or repetitive, SMEs will be able to charge a fee for providing access.
- **Impact Assessments**: SMEs will have no obligation to carry out an impact assessment unless there is a specific risk.

The rules will also be **flexible**. The EU rules will adequately and correctly take into account risk. We want to make sure that obligations are not imposed except where they are necessary to protect personal data: the baker on the corner will not be subject to the same rules as a (multinational) data processing specialist. In a number of cases, the obligations of data controllers and processors are calibrated to the size of the business and to the nature of the data being processed. For example, SMEs will not be fined for a first and non-intentional breach of the rules.

3. What are the "one-stop shop" and the "consistency mechanism" proposed in the EU data protection reform? How will they help?

Within a single market for data, identical rules on paper will not be enough. We have to ensure that the rules are interpreted and applied in the same way everywhere. That is why our reform introduces a **consistency mechanism** to streamline cooperation between the data protection authorities on issues with implications for all of Europe.

At present, a company processing data in the EU has to deal with 28 national laws and with even more national and local regulators. The Data Protection Regulation will establish a single, Europe-wide law for data protection, replacing the current inconsistent patchwork of 28 national laws. It will also create a regulatory **"one-stop-shop"** for business: companies will only have to deal with one supervisory authority, not 28.

The flaws of the present system were illustrated in the Google Street View case. The actions of a single company affected individuals in several Member States in the same way. Yet they prompted uncoordinated and divergent responses from national data protection authorities.

The one-stop shop will ensure legal certainty for businesses operating throughout the EU and bring benefits for individuals and data protection authorities.

Businesses will profit from faster decisions, from one single interlocutor (eliminating multiple contact points), and from less red tape. They will benefit from consistency of decisions where the same processing activity takes place in several Member States.

At the same time, individuals will see their protection enhanced via their local supervisory authorities, because **individuals will always be able to go to their local data protection authority**. The aim is to improve the current system in which individuals living in one Member State have to travel to another Member States to lodge a complaint with a data protection authority just because the company is based outside their home country. **At the moment, when a business is established in one Member State, only the Data Protection Authority of that Member State is competent, even if the business is processing data across Europe**. The proposals aim to correct this anomaly.

The new rules bring the resolution of a complaint closer to home for citizens, simplifying procedures and removing complexity, and thereby making problems easier and faster to resolve. This would decisively help citizens in cases similar to that of the Austrian student, who had to file his complaint against Facebook in English before the authority in Ireland, where Facebook is established.

The proposals also enshrine the right of a citizen to take a company processing his data to court in his home Member State. Every citizen therefore has rights of administrative and judicial redress at home.

4. How will the EU data protection help the EU Digital Single Market?

The world has changed profoundly since 1995, the year the existing EU data protection framework was adopted. Technological revolutions have led to an explosion in the quantity and quality of personal data available in the Digital Single Market. Companies have learnt to harness its potential in sectors as diverse as insurance, health and advertising. Collected, analysed and moved by these companies, personal data has acquired enormous economic value. **According to the Boston Consulting Group, the value of EU citizens' data was €315 billion in 2011 and has the potential to grow to nearly €1 trillion in 2020.**

The data protection reform will help the Digital Single Market realise this potential. The benefits of simplification via the EU data protection reform are estimated at €2.3 billion per year.

The biggest challenge to growth in personal data-dependent industries is a lack of trust. Only if people are willing to give out their personal data will companies reap the full rewards of our digital single market. At the moment, people's trust in the way private companies handle their data is declining.

Data protection has an important part to play in addressing this lack of trust. People need to see that their rights are enforced in a meaningful way. The reform will update citizen's rights such as the right to be forgotten, the right to data portability and the right to be informed of personal data breaches (see above). The reform will also ensure that the Union's rules are properly applied. It provides for an effective enforcement mechanism and empowers national regulators to impose fines of up to 2% of a company's annual worldwide turnover.

5. What is the right to be forgotten? Will it affect the freedom of the press and historical archives?

The Commission's 2012 proposals include a reinforced Right to be Forgotten. The reform proposals build on the existing right to demand that personal data should be deleted if it is no longer needed for any legitimate purpose. This covers all kinds of everyday situations. For example, children may not understand the risks involved in making their personal information available – only to regret it when they grow up. They should be able to delete that information if they want to.

The right to be forgotten is not about rewriting history. The Commission's proposal protects freedom of expression and the freedom of the media, as well as historical and scientific research. It provides exemptions for these sectors asking Member States to adopt national laws to guarantee the respect of these fundamental rights. This allows archives to continue operating on the basis of the same principles as today. Equally, personal data may be kept for as long as it is needed to carry out a contract or to meet a legal obligation (for example when citizens have a loan contract with their bank). **In short, the right to be forgotten is not absolute and does not affect historical research or the freedom of the press.**

The rights of businesses are also protected. If the personal data in question has been made public (for example, posted on the Internet), a company must make a genuine effort to ensure third parties know about the citizen's request to delete the data. Evidently a company will not be obliged to wipe out every trace left in search indexes and that is not what the Commission is asking for. Companies should simply take reasonable steps to ensure that third parties, to whom the information has been passed on, are informed that the individual would like it deleted. In most cases this will involve nothing more than writing an email.

6. How will the EU data protection reform affect scientific research?

Scientific research in the EU stands to benefit from the proposed data protection reform. Personal data relating to health are sensitive data and should generally not be processed, unless this is necessary for reasons of public interest, or where the identified person has given his approval. The data protection rules we have in Europe at the moment do not harmonise conditions for health data processing. This has resulted in fragmentation, costs and disincentives for scientists and businesses involved.

The Commission's reform package aims at eliminating fragmentation and providing consistency and coherence for the whole of the Union. This should in particular benefit the research sector. The General Data Protection Regulation has specific provisions on processing for health purposes and on historical, statistical and scientific research purposes. These provisions will be fully harmonised – providing one set of rules on research data across the Union.

The right to be forgotten does not apply to these sectors.

The uniformity of the rules will reduce costs and complexity, and act as a strong driver for the development of cross-border healthcare services, public-private health initiatives and eHealth applications that crucially depend on the processing of personal data.

7. What is the EU response to allegations of surveillance of European citizens by US intelligence agencies?

Trust across the transatlantic relationship has been damaged by the revelations. The European Commission responded to the U.S. surveillance programmes by making clear that the mass surveillance of citizens is unacceptable. Data collection should be targeted and be limited to what is proportionate to the objectives that have been set. National security does not mean that anything goes.

The surveillance revelations also have an economic impact. A survey carried out by the Cloud Security Alliance after the recent surveillance revelations found that 56% of respondents were hesitant to work with any U.S.-based cloud service provider. That is the impact of consumer mistrust. In monetary terms, the Information Technology and Innovation Foundation estimates that the surveillance revelations will cost the U.S. cloud computing industry $22 to $35 billion in lost revenues over the next three years. **In short: lost trust means lost revenue.**

The European Union's response

In November 2013, the European Commission set out the actions that need to be taken in order to restore trust in data flows between the EU and the U.S. (IP/13/1166). The Commission's response took the form of (1) a strategy paper (a Communication) on transatlantic data flows setting out the challenges and risks following the revelations of U.S. intelligence collection programmes, as well as the steps that need to be taken to address these concerns; (2) an analysis of the functioning of 'Safe Harbour', which regulates data transfers for commercial purposes between the EU and U.S.; and (3) a report on the findings of the EU-U.S. Working Group (see MEMO/13/1059) on Data Protection which was set up in July 2013.

The Commission's strategy paper called for action in six areas:

- **A swift adoption of the EU's data protection reform**: the strong legislative framework with clear rules that are enforceable also in situations when data is transferred and processed abroad is, more than ever, a necessity.
- **Making Safe Harbour safer**: the Commission made 13 recommendations to improve the functioning of the Safe Harbour scheme, after an analysis found the functioning of the scheme deficient in several respects. Remedies should be identified by summer 2014. The Commission will then review the functioning of the scheme based on the implementation of these 13 recommendations and decide on the future of Safe Harbour.
- **Strengthening data protection safeguards in the law enforcement area**: the current negotiations on an EU-U.S. "umbrella agreement" (IP/10/1661) for transfers and processing of data in the context of police and judicial cooperation should be concluded swiftly. An agreement must guarantee a high level of protection for citizens who should benefit from the same rights on both sides of the Atlantic. Notably, EU citizens not resident in the U.S. should benefit from judicial redress mechanisms. At the last EU-U.S.-Justice and Home Affairs Ministerial Meeting (of 18 November) good progress was made (MEMO/13/1010).

- **Using the existing Mutual Legal Assistance and Sectoral agreements to obtain data**: The U.S. administration should commit to, as a general principle, making use of a legal framework like the mutual legal assistance and sectoral EU-U.S. Agreements such as the Passenger Name Records Agreement and Terrorist Financing Tracking Programme whenever transfers of data are required for law enforcement purposes. Asking the companies directly should only be possible under clearly defined, exceptional and judicially reviewable situations.
- **Addressing European concerns in the on-going U.S. reform process**: The European Commission welcomed President Obama's remarks and presidential directive on the review of U.S. intelligence programmes (MEMO/14/30). It particularly welcomed the willingness of President Obama to extend safeguards currently available to U.S. citizens as regards data collection for national security purposes to non U.S.-citizens. These commitments should now be followed by legislative action.
- **Promoting privacy standards internationally**: The U.S. should accede to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), as it acceded to the 2001 Convention on Cybercrime.

The Commission also made clear that standards of data protection will **not** be part of the on-going negotiations for a Transatlantic Trade and Investment Partnership.

The EU-U.S. Working Group

The ad hoc EU-U.S. Working Group on data protection was established in July 2013 to examine issues arising from revelations of a number of U.S. surveillance programmes involving the large-scale collection and processing of personal data. The purpose was to establish the facts around U.S. surveillance programmes and their impact on personal data of EU citizens.

The main findings of the Working Group were the following:

- A number of **U.S. laws allow the large-scale collection and processing of personal data** that has been transferred to the U.S. or is processed by U.S. companies, **for foreign intelligence purposes**. The U.S. confirmed the existence and the main elements of certain aspects of these programmes, under which data collection and processing is done with a basis in U.S. law laying down specific conditions and safeguards.
- **There are differences in the safeguards applicable to EU citizens compared to U.S. citizens whose data is processed.** There is a lower level of safeguards which apply to EU citizens, as well as a lower threshold for the collection of their personal data. While U.S. citizens benefit from constitutional protections these do not apply to EU citizens not residing in the U.S.
- Since the orders of the Foreign Intelligence Surveillance Court are secret and companies are required to maintain secrecy with regard to the assistance they are required to provide, there are no avenues (judicial or administrative), for either EU or U.S. data subjects to be informed of whether their personal data is being collected or further processed. **There are no opportunities for individuals to obtain access, rectification or erasure of data, or administrative or judicial redress.**

- While there is a degree of oversight by the three branches of Government which applies in specific cases, including judicial oversight for activities that imply a capacity to compel information, **there is no judicial approval for how the data collected is queried:** judges are not asked to approve the 'selectors' and criteria employed to examine the data and mine usable pieces of information.

Making Safe Harbour safer

The European Commission made 13 recommendations to improve the functioning of the Safe Harbour scheme. The Commission specifically called on U.S. authorities to identify remedies by summer 2014. The Commission will then review the functioning of the Safe Harbour scheme based on the implementation of these 13 recommendations and decide on its future.

The 13 Recommendations are (see also MEMO/13/1059):

Transparency

1. Self-certified companies should publicly disclose their privacy policies.
2. Privacy policies of self-certified companies' websites should always include a link to the Department of Commerce Safe Harbour website which lists all the 'current' members of the scheme.
3. Self-certified companies should publish privacy conditions of any contracts they conclude with subcontractors, e.g. cloud computing services.
4. Clearly flag on the website of the Department of Commerce all companies which are not current members of the scheme.

Redress

5. The privacy policies on companies' websites should include a link to the alternative dispute resolution (ADR) provider.
6. ADR should be readily available and affordable.
7. The Department of Commerce should monitor more systematically ADR providers regarding the transparency and accessibility of information they provide concerning the procedure they use and the follow-up they give to complaints.

Enforcement

8. Following the certification or recertification of companies under Safe Harbour, a certain percentage of these companies should be subject to ex officio investigations of effective compliance of their privacy policies (going beyond control of compliance with formal requirements).
9. Whenever there has been a finding of non-compliance, following a complaint or an investigation, the company should be subject to follow-up specific investigation after 1 year.
10. In case of doubts about a company's compliance or pending complaints, the Department of Commerce should inform the competent EU data protection authority.
11. False claims of Safe Harbour adherence should continue to be investigated.

Access by US authorities

12. Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.
13. It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate.

EU-U.S. negotiations on a data protection 'umbrella agreement'

The EU and the U.S. are currently negotiating a framework agreement on data protection in the field of police and judicial cooperation ("umbrella agreement") (IP/10/1661). The EU's objective in these negotiations is to ensure a high level of data protection, in line with the EU data protection rules, for citizens whose data is transferred across the Atlantic, thereby further strengthening EU-U.S. cooperation in the fight against crime and terrorism.

The conclusion of such an agreement, providing for a high level of protection of personal data, would represent a major contribution to strengthening trust across the Atlantic.

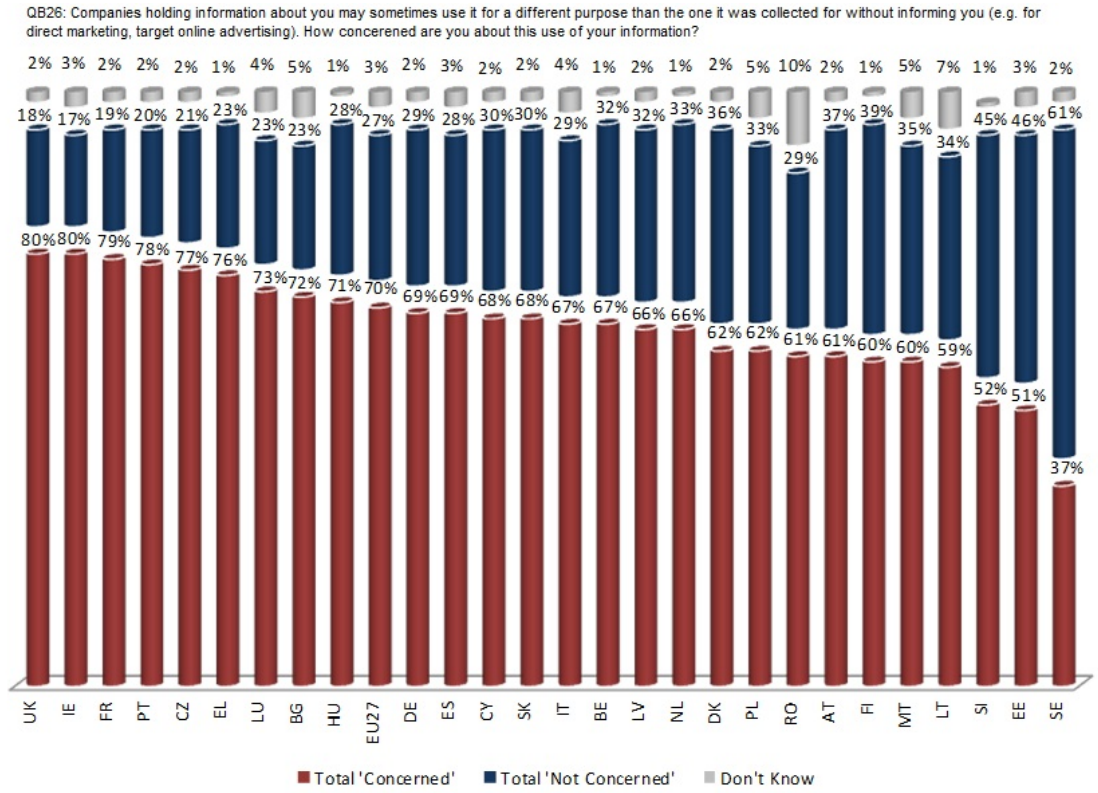
At the last EU-U.S.-Justice and Home Affairs Ministerial Meeting (of 18 November) we made good progress:

- First, the U.S. committed to working to resolve one of the outstanding issues for the EU – namely to give EU citizens who are not resident in the U.S. the right to judicial redress if their data has been mishandled.
- Second, the U.S. underlined their commitment to use the EU-U.S. Mutual Legal Assistance Agreement more broadly and effectively when they want to obtain data of EU citizens for evidence purposes in criminal proceedings.

The EU and U.S. committed to "complete the negotiations on the agreement ahead of summer 2014" (MEMO/13/1010).

ANNEX

1. Eurobarometer: Seven Europeans out of ten are concerned about the potential use that companies may make of the information disclosed.



Source: Flash Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union, June 2011

For more information

Press release

Reding speech at CEPS

Press pack: data protection reform:

http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

European Commission – data protection: http://ec.europa.eu/justice/data-protection

Homepage of Vice-President Viviane Reding, EU Justice Commissioner:

http://ec.europa.eu/reding

Justice Directorate General Newsroom:

http://ec.europa.eu/justice/newsroom/index_en.htm

Follow the Vice-President on Twitter:@VivianeRedingEU

Follow EU Justice on Twitter: @EU_Justice