Questions and Answers – Data protection reform package

The reform is an essential step to strengthening citizens' fundamental rights in the digital age and facilitating business by simplifying rules for companies in the Digital Single Market.

What will change under the General Data Protection Regulation?

The Regulation updates and modernises the principles enshrined in the 1995 Data Protection Directive to guarantee privacy rights. It focuses on:

- reinforcing individuals' rights;
- strengthening the EU internal market;
- ensuring stronger enforcement of the rules;
- streamlining international transfers of personal data and;
- setting global data protection standards.

The changes will give people **more control** over their personal data and make it easier to access it. They are designed to make sure that people's personal information is protected – no matter where it is sent, processed or stored – even outside the EU, as may often be the case on the internet.

What are the benefits for citizens?

The reform provides tools for **gaining control of one's personal data**, the protection of which is a fundamental right in the European Union. The data protection reform **will strengthen citizens' rights and build trust**.

Nine out of ten Europeans have expressed concern about mobile apps collecting their data without their consent, and seven out of ten worry about the potential use that companies may make of the information disclosed. The new rules address these concerns through:

- **A "right to be forgotten"**: When an individual no longer wants her/his data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted. This is about protecting the privacy of individuals, not about erasing past events or restricting freedom of the press.
- **Easier access to one's data**: Individuals will have more information on how their data is processed and this information should be available in a clear and understandable way. A **right to data portability** will make it easier for individuals to transmit personal data between service providers.
- **The right to know when one's data has been hacked**: Companies and organisations must notify the national supervisory authority of data breaches which put individuals at risk and communicate to the data subject all high risk breaches as soon as possible so that users can

take appropriate measures.

- **Data protection by design and by default**: 'Data protection by design' and 'Data protection by default' are now essential elements in EU data protection rules. Data protection safeguards will be built into products and services from the earliest stage of development, and privacy-friendly default settings will be the norm – for example on social networks or mobile apps.

Right to be forgotten: How will it work?

Already the current Directive gives individuals the possibility to have their data deleted, in particular when the data is no longer necessary. For example, if an individual has given her or his consent to processing for a specific purpose (such as display on a social networking site) and does not want this service anymore, then there is no reason to keep the data in the system.

In particular, when children have made data about themselves accessible – often without fully understanding the consequences – they must not be stuck with the consequences of that choice for the rest of their lives.

This does not mean that on each request of an individual all his personal data are to be deleted at once and forever. If, for example, the retention of the data is necessary for the performance of a contract, or for compliance with a legal obligation, the data can be kept as long as necessary for that purpose.

The proposed provisions on the "right to be forgotten" are very clear: **freedom of expression,** as well as historical and scientific **research are safeguarded**. For example, no politician will be able to have their earlier remarks deleted from the web. This will thus allow, inter alia, news websites to continue operating on the basis of the same principles.

Is there specific protection for children?

Yes, the Regulation recognises that children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. For instance, they benefit from a clearer right to be forgotten.

When it comes to information society services offered directly to a child, the Regulation foresees that consent for processing the data of a child must be given or authorised by the holder of the parental responsibility over the child. The age threshold is for Member States to define within a range of 13 to 16 years.

The aim of this specific provision aims at protecting children from being pressured to share personal data without fully realising the consequences. It will not to stop teenagers from using the Internet to get information, advice, education etc. Moreover, the Regulation specifies that the consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

What are the benefits for businesses?

The reform provides **clarity and consistency of the rules to be applied, and restores trust of the consumer**, thus allowing undertakings to seize fully the opportunities in the Digital Single Market.

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. By strengthening Europe's high standards of data protection, lawmakers are creating business opportunities.

The data protection reform package helps the Digital Single Market realise this potential through:

- **One continent, one law**: 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**: 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.
- **The same rules for all companies – regardless of where they are established**: Today European companies have to adhere to stricter standards than companies established outside the EU but also doing business in our Single Market. With the reform, companies based outside of Europe will have to apply the same rules when they offer goods or services on the EU market. This creates a level playing field.
- **Technological neutrality**: the Regulation enables innovation to continue to thrive under the new rules.

What is the one-stop shop?

Within a single market for data, identical rules on paper are not enough. The rules must be applied in the same way everywhere. The 'one-stop-shop' will streamline cooperation between the data protection authorities on issues with implications for all of Europe. Companies will only have to deal with one authority, not 28. It will ensure legal certainty for businesses. 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. **Individuals will have more control.**

How will that help business?

The new right to **data portability** will allow individuals to move their personal data from one service provider to another. Start-ups and smaller companies will be able to access data markets dominated by digital giants and attract more consumers with privacy-friendly solutions. This will make the

European economy more competitive.

Example: Benefits for individuals, benefits for businesses

A new small company wishes to enter the market offering an online social media sharing website. The market already has big players with a large market share. Under the current rules, each new customer will have to consider starting over again with the personal data they wish to provide to be established on the new website. This can be a disincentive for some people considering switching to the new business.

***With the Data Protection Reform:** The right to data portability will make it easier for potential customers to transfer their personal data between service providers. This allows customers to exercise control over their personal data, and at the same time fosters competition and encourages new businesses in the marketplace.*

What are the benefits for SMEs?

The data protection reform is geared towards **stimulating economic growth** by cutting costs and red tape for European business, also for small and medium enterprises (SMEs). By having one rule instead of 28, the EU's data protection reform will help SMEs break into new markets. In a number of cases, the obligations of data controllers and processors are calibrated to the size of the business and/or to the nature of the data being processed. For example:

- **SMEs need not appoint a data protection officer** unless their core activities require regular and systematic monitoring of the data subjects on a large scale, or if they process special categories of personal data such as that revealing racial or ethnic origin or religious beliefs. Moreover, this will not need to be a full-time employee but could be an ad-hoc consultant, and therefore, would be much less costly.
- **SMEs need not keep records of processing activities** unless the processing they carry out is not occasional or likely to result in a risk for the rights and freedoms of data subject.
- **SMEs will not be under an obligation to report all data breaches to individuals**, unless the breaches represent a high risk for their rights and freedoms.

How will the new rules save money?

The Regulation will establish a single, pan-European law for data protection meaning that companies can simply deal with one law, not 28. The new rules will bring benefits of an estimated **€2.3 billion per year**.

Example: Cutting costs

A chain of shops has its head office in France and franchised shops in 14 other EU countries. Each shop collects data relating to clients and transfers

it to the head office in France for further processing.

With the current rules: *France's data protection laws would apply to the processing done by head office, but individual shops would still have to report to their national data protection authority, to confirm they were processing data in accordance with national laws in the country where they were located. This means the company's head office would have to consult local lawyers for all its branches to ensure compliance with the law. The total costs arising from reporting requirements in all countries could be over €12,000.*

With the Data Protection Reform: *The data protection law across all 14 EU countries will be the same – one European Union – one law. This will eliminate the need to consult with local lawyers to ensure local compliance for the franchised shops. The result is direct cost savings and legal certainty.*

How will the Data Protection Reform encourage innovation and use of big data?

According to some estimates, the value of European citizens' personal data could grow to nearly €1 trillion annually by 2020. The new EU rules will offer flexibility to businesses all while protecting individuals' fundamental rights.

'Data protection by design and by default' will become an essential principle. It will incentivise businesses to innovate and develop new ideas, methods, and technologies for security and protection of personal data. Used in conjunction with data protection impact assessments, businesses will have effective tools to create technological and organisational solutions.

The Regulation promotes techniques such as **anonymisation** (removing personally identifiable information where it is not needed), **pseudonymisation** (replacing personally identifiable material with artificial identifiers), and **encryption** (encoding messages so only those authorised can read it) to protect personal data. This will encourage the use of "big data" analytics, which can be done using anonymised or pseudonymised data.

Example: Driverless cars

The driverless cars technology requires important data flows, including the exchange of personal data. Data protection rules go hand in hand with innovative and progressive solutions. For example, in case of a crash, cars equipped with eCall emergency call system can automatically call the nearest emergency centre. This is an example of a workable and efficient solution in line with EU data protection principles.

With the new rules, the function of eCall will become easier, simpler and more efficient in terms of data protection. It is a data protection principle that when personal data is collected for one or more purposes it should not be further processed in a way that is incompatible with the original purposes. This does not prohibit processing for a different purpose or restrict 'raw data' for use in analytics.

A key factor in deciding whether a new purpose is incompatible with the original purpose is whether it is fair. Fairness will consider factors such as; the effects on the privacy of individuals (e.g. specific and targeted decisions about identified persons) and whether an individual has a reasonable expectation that their personal data will be used in the new way.

So in the case of driverless cars, raw data can be used to analyse where the most accidents take place and how future accidents could be avoided. It can also be used to analyse traffic flows in order to reduce traffic jams.

Businesses should be able to anticipate and inform individuals of the potential uses and benefits of big data – even if the exact specifics of the analysis are not yet known. Businesses should also think whether the data can be anonymised for such future processing. This will allow raw data to be retained for big data, while protecting the rights of individuals.

The new data protection rules provide businesses with opportunities to remove the lack of trust that can affect people's engagement with innovative uses of personal data. Providing individuals with clear, effective information will help build trust in analytics and innovation. The information to be provided is not exactly how the data is to be processed, but the purposes for which it will be processed.

The apparent complexity of innovated products and big data analytics is not an excuse for failing to seek consent of people where it is required. However, consent is not the only basis for processing.

Companies are free to base processing on a contract, on a law or, on, in the absence of other bases, on a "balancing of interests". These 'formal requirements', such as consent, are set out in the rules to provide the necessary control by individuals over their personal data and to provide legal certainty for everyone. The new EU rules will provide flexibility on how to meet those requirements.

How will the European Data Protection Board work?

Currently all European data protection authorities meet under the "Article 29 Working Party", as set up under Article 29 of the Data Protection Directive (Directive 95/46/EC). This body will be replaced by the European Data Protection Board (EDPB), which will be composed of representatives from the national data protection authority of each EU Member State, the European Data Protection Supervisor and the Commission (without voting right). The EDBP Chair will be chosen from among its members. In the same way as the Article 29 Working Party, the EDPB will monitor the correct application of the new data protection rules, advise the European Commission on any relevant issue, and give advice and guidance on a variety of topics related to data protection. The novelty of the GDPR is that the EDPB will also issue binding decisions in the case of certain disputes between national data protection authorities thus fostering the consistent application of data protection rules throughout the EU.

What penalties will there be for businesses if they break the new data

protection rules?

The General Data Protection Regulation establishes a range of tools for enforcing the new rules, including penalties and fines. When it comes to deciding on an appropriate fine, each case will be carefully assessed and a range of factors will be taken into account:

- the gravity/ duration of the violation;
- the number of data subjects affected and level of damage suffered by them;
- the intentional character of the infringement;
- any actions taken to mitigate the damage;
- the degree of co-operation with the supervisory authority.

The regulation sets two ceilings for fines if the rules are not respected. The first ceiling sets fines up to a maximum of €10 million or, in case of an undertaking, up to 2% of worldwide annualturnover. This first category of fine would be applied for instance if a controllers does to conduct impact assessments, as required by the Regulation. The higher ceiling of fines reaches up to a maximum of €20 million or 4% of worldwide annual turnover. An example would be an infringement of the data subjects' rights under the Regulation. Fines are adjusted according to the circumstances of each individual case.

How does the GDPR protect personal data in case of cyberattacks?

- **The GDPR contains an obligation that personal data should be processed in a manner that ensures appropriate security of personal data**, including for preventing unauthorised access to or use of personal data and the equipment used for the processing. Therefore, the controller or processor should evaluate the risks inherent in the processing of personal data and implement measures to mitigate those risks. (Art. 32 of the GDPR)
- **Data controllers will need to inform data subjects about data breaches without undue delay.** This obligation will be relevant where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. (Article 33 of the GDPR)
- **Data controllers will also have to notify the relevant data protection supervisory authority, unless the controller is able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.** Such notifications shall be submitted without undue delay and, where feasible, in general not later than 72 hours after having data controllers become aware of it. (Article 34 of the GDPR)
- **The GDPR contains clear rules on conditions for imposing administrative fines.** Data protection authorities will be able to fine companies who do not comply with EU rules, if they have for instance not informed their clients that they're data have been breached or the data protection authorities.

How will the new rules work in practice?

Example:*a multinational company with several establishments in EU Member States has an online navigation and mapping system across Europe. This system collects images of all private and public buildings, and may also take pictures of individuals.*

With the current rules: *The data protection safeguards upon data controllers vary substantially from one Member State to another. In one Member State, the deployment of this service led to a major public and political outcry, and some aspects of it were considered to be unlawful. The company then offered additional guarantees and safeguards to the individuals residing in that Member State after negotiation with the competent DPA, however the company refused to commit to offer the same additional guarantees to individuals in other Member States. Currently, data controllers operating across borders need to spend time and money (for legal advice, and to prepare the required forms or documents) to comply with different, and sometimes contradictory, obligations.*

With the new rules: *The new rules will establish a single, pan-European law for data protection, replacing the current inconsistent patchwork of national laws. Any company – regardless of whether it is established in the EU or not – will have to apply EU data protection law should they wish to offer their services in the EU.*

Example: *a small advertising company wants to expand its activities from France to Germany.*

With the current rules: *Its data processing activities will be subject to a separate set of rules in Germany and the company will have to deal with a new regulator. The costs of obtaining legal advice and adjusting business models in order to enter this new market may be prohibitive. For example, some Member States charge notification fees for processing data.*

With the new rules: *The new data protection rules will scrap all notification obligations and the costs associated with these. The aim of the data protection regulation is to remove obstacles to cross-border trade.*

What about the Data Protection Directive for the police and criminal justice sector?

The Police Directive ensures the protection of personal data of individuals involved in criminal proceedings, be it as witnesses, victims, or suspects. It will also facilitate a smoother exchange of information between Member States' police and judicial authorities, improving cooperation in the fight against terrorism and other serious crime in Europe. It establishes a comprehensive framework to ensure a high level of data protection whilst taking into account the specific nature of the police and criminal justice field.

How does the Data Protection Directive for the police and criminal justice sector impact law enforcement operations?

Law enforcement authorities will be able to **exchange data more efficiently and effectively.** By further harmonising the 28 different national legislations, the common rules on data protection will enable law enforcement and judicial authorities to cooperate more effectively and more rapidly with each other. It will facilitate the exchange of personal data necessary to prevent crime under conditions of legal certainty, fully in line with the Charter of Fundamental Rights.

Criminal law enforcement authorities will no longer have to apply different sets of data protection rules according to the origin of the personal data, **saving time and money**.

The new rules will apply to both domestic processing and cross-border transfers of personal data. Having more harmonised laws in all EU Member States will make it easier for our police forces to work together. The rules in the Directive take account the specific needs of criminal law enforcement and respect the different legal traditions in Member States.

How does the Directive affect citizens?

Individuals' personal data will be better protected. The Directive **protects citizens' fundamental right** to data protection when data is used by criminal law enforcement authorities. Everyone's personal data should be processed lawfully, fairly, and only for a specific purpose. All law enforcement processing in the Union must comply with the principles of necessity, proportionality and legality, with appropriate safeguards for the individuals. Supervision is ensured by independent national data protection authorities and effective judicial remedies must be provided.

The Directive also provides **clear rules for the transfer of personal data** by criminal law enforcement authorities outside the EU, to ensure that these transfers take place with an adequate level of data protection. The directive provides robust rules on personal data exchanges at national, European and international level.

How does the Directive affect the work of criminal law enforcement?

Having the same law in all EU Member States will make it **easier for our criminal law enforcement authorities to work together** in exchanging information. This will increase the efficiency of criminal law enforcement and thus create conditions for more effective crime prevention.

This is also why the Data Protection Directive is considered a **key element** of the development of the EU's area of freedom, security and justice and a building block of the EU Agenda on Security. The Directive replaces Framework Decision 2008/977/JHA which previously governed data processing by police and judicial authorities.

The entry into force of the Lisbon Treaty and, in particular, the introduction of a new legal basis (Article 16 TFEU) allows the establishment of a comprehensive data protection framework in the area of police and judicial cooperation in criminal matters. The new framework will cover both

cross-border and domestic processing of personal data.

For more information

Statement/17/1436