European Commission – Fact Sheet
欧州委員会 – 概況報告

Questions and Answers - Data protection reform package

データ保護改革包括案に関する質疑応答

Brussels, 24 May 2017
2017 年 5 月 24 日ブリュッセル

The data protection reform package which entered into force in May 2016 and will be applicable as of May 2018 includes the General Data Protection Regulation ("Regulation") and the Data Protection Directive for the police and criminal justice sector.
2016 年 5 月に制定し、2018 年 5 月時点で適用されるデータ保護改革包括案には、一般データ保護規則（以下、「規則」という。）と警察及び刑事司法部門のデータ保護指令が含まれます。

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.
この改革は、デジタル時代における市民の基本的権利を強化し、デジタル単一市場における企業の規則を簡素化することによってビジネスを促進するための不可欠なステップです。

What will change under the General Data Protection Regulation?
一般データ保護規則では何が変更されますか？

The Regulation updates and modernises the principles enshrined in the 1995 Data Protection Directive to guarantee privacy rights. It focuses on:
規則は、プライバシーの権利を保障するため、1995 年のデータ保護指令に定められた原則を更新し、最新のものとします。以下の点に重点を置いています。

- reinforcing individuals' rights;
- 個人の権利の強化
- strengthening the EU internal market;
- EU 域内市場の強化
- ensuring stronger enforcement of the rules;
- 規則の強化の保証
- streamlining international transfers of personal data and;
- 個人データの国際移転の簡素化
- setting global data protection standards.
- グローバルなデータ保護水準の設定

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.
この変更により、人々は個人データをより制御できるようになり、個人データにアクセスしやすくなります。インターネット上でよくあるように、移転、処理、保存される場所に関係なく、それが EU 域外であっても、個人情報が確実に保護されるようデザインされます。

What are the benefits for citizens?
市民にとっての利点は何ですか？

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**.
改革は個人データを制御する手段を提供します。その保護は EU における基本的権利です。データ保護改革は市民の権利を強化し、信頼を築くことでしょう。

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:
欧州の人々の 10 人中 9 人は、モバイルアプリが本人の同意無しに彼らのデータを収集することについて懸念を表明し、10 人中 7 人は、開示された情報を企業が利用する可能性を心配しています。新しい規則は、これらの懸念について以下の方法で対処します。

- **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.
- 「忘れられる権利」:本人がもう自分のデータを処理されることを望まず、それを保持する正当な根拠がない場合、データは削除されます。これは、個人のプライバシーの保護であり、過去の出来事の消去や、報道の自由の制限にはあたりません。
- **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.
- データへのアクセスの容易性:本人がデータの処理方法についてより情報を持ち、明確に、分かりやすい方法でその情報を入手可能になっているべきです。データポータビリティの権利は、本人がサービスプロバイダ間で個人データを送付しやすくするでしょう。

- **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.
- **個人のデータがハッキングされた時に知る権利**：企業・組織等は本人にリスクが及ぶデータ違反について国の監督機関への届出が義務付けられ、また、利用者が適切な措置を講じられるよう、できるだけ早く全ての高リスクの違反をデータ対象者へ通知する必要があります。
- **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.
- **データ保護バイデザイン及びデータ保護バイデフォルト**：「データ保護バイデザイン」及び「データ保護バイデフォルト」は今や EU におけるデータ保護規則の基本的要素である。例えばソーシャルネットワークやモバイルアプリのように、開発の初期段階からデータ保護手段が製品やサービスに組み込まれ、プライバシーを侵害しない初期設定が基準となっていくでしょう。

Right to be forgotten: How will it work?
忘れられる権利：

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.
既に現行の指令でも、個人がデータを削除することは可能で、特に、データが不要になった場合に使用します。例えば、特定の目的（ソーシャルネットワークのサイトへの表示等）のための処理に個人が同意した場合で、このサービスがもう不要となった場合には、システムにそのデータを保存する理由はありません。

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.
特に、子どもが（大抵の場合、その影響を十分に理解することなく）彼ら自身のデータについてアクセスできるようにした場合、残りの人生をその選択の結果に悩まされようになってはいけません。

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.
これは、個人の要請があり次第、その全個人データが一度に、永久に削除されることを意味するものではありません。もし、例えば、データ保有が契約の履行又は法的義務の遵守のために必要な場合、データはその目的の達成に必要な期間、保管することができます。

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.
「忘れられる権利」の規定で提案されていることは非常に明確です。表現の自由は、歴史的、科学的研究と同様に保護されます。例えば、どの政治家も以前の発言を Web から削除することはできません。従って、特にニュースウェブサイトは、同じ原則に基づき運用を継続することが可能となります。

Is there specific protection for children?
子どもに対して特別に保護していますか？

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.
はい。規則は、子どもは個人データの処理に関してリスクや影響、保護手段、彼らの権利を認識していない可能性があるため、子どもには個人データの特別の保護が必要であるとしています。例えば、より明確になった「忘れられる権利」の恩恵を得られます。

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.
子どもに直接提供される情報社会サービスについては、子どものデータ処理に関する同意は子どもの親権者によって認可されなければならないと規則は見越しています。EU 加盟国におけるしきい値となる年齢の範囲は 13 歳から 16 歳までと明確にされています。

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.

この特別規定は、影響を十分に理解しないまま個人データを共有させるよう圧力をかけられることから子どもを保護することを目的としています。十代の若者が情報や助言、教育等を得るためにインターネットを利用することを妨げるものではありません。更に規則は、子どもに直接提供される予防又はカウンセリングのサービスに関しては、親権者の同意が必要でないことを明記しています。

What are the benefits for businesses?
事業にとっての利点は何ですか？

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.
この改革は、ルール適用における明快さと一貫性をもたらし、消費者の信頼を回復させ、デジタル単一市場における機会を十分に奪回できるようにします。

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.
データは今日のデジタル経済における貨幣です。収集され、分析され、世界中を移動した個人データは巨大な経済的重要性を帯びつつあります。ある見積もりによると、欧州の市民の個人データの価値は、2020 年までに年間約 1 兆ユーロに増加する可能性があります。欧州の高いデータ保護基準を強化することによって、議員等はビジネスチャンスを創出しています。

The data protection reform package helps the Digital Single Market realise this potential through:
データ保護改革包括案は、以下のことを通して、デジタル単一市場がこの可能性を実現するのに役立ちます。

- **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.
- 一つの大陸に一つの法：現行の一貫性のない各国法の寄せ集めに置き換わる、全欧州で唯一のデータ保護法です。企業は（EU 加盟国数の）28 ではなく、1 つの法律を扱うこととなり、その利益は年間 23 億ユーロと推定されます。
- **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.

- ワンストップショップ：事業にとっての「ワンストップショップ（1ヶ所で全てが済む総合店舗）」です。企業は、（EU（加盟国数の）28 ではなく、ただ 1 つの監督局で手続するだけとなり、EU における事業がより簡単で安価になります。
- **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.
- 設立場所に関わらない、全企業にとって同一のルール：今日の欧州の企業は、我々の単一市場で事業を行う EU 域外で設立された企業よりも厳しい基準を遵守しなければなりません。この改革では、欧州域外に拠点を置く企業が EU 市場で商品やサービスを提供する際に、同じ規則を適用することになります。これは平等な競争の場を作り出します。
- **Technological neutrality**: the Regulation enables innovation to continue to thrive under the new rules.
- 技術的な中立性：規則は、新しいルールの下で技術革新が進展し続けることを可能にします

What is the one-stop shop?
ワンストップショップとは何ですか？

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.**
データの単一市場内では、理論上同一のルールというだけでは不充分です。ルールはどこでも同じように適用されなくてはなりません。「ワンストップショップ」は、欧州全土に影響を及ぼす問題におけるデータ保護機関間の協力を効率よくします。企業が手続しなくてはならないのは（EU 加盟国数の）28 ではなく、ただ 1 つの機関です。それは事業にとっての法的確実性を保証します。事業は、より早い判定、（多くの連絡先がなくなり）唯一の代弁者、官僚的で面倒な手続きの減少により利益を得ます。幾つかの加盟国で同じ処理が行われる場合、判定の一貫性の恩恵も受けます。個人は更に制御が可能となります。

How will that help business?
事業にどのように役立つのでしょうか？

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.
新しいデータポータビリティの権利は、個人が彼らの個人データをあるサービスプロバイダから別のサービスプロバイダに移すことを可能とします。新興企業や中小企業は、巨大デジタル企業が支配するデータ市場にアクセスし、プライバシー保護に適したソリューションを以てより多くの消費者を得ることができます。これにより欧州経済はより競争力のあるものになります。

Example: Benefits for individuals, benefits for businesses
例：個人の利益、企業の利益

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.
新しい中小企業がインターネット上のソーシャルメディア共有ウェブサイトを提供する市場に参入したいとします。市場には既に大きな市場シェアを持つ巨大企業が存在します。現行のルールでは、新規顧客は、新しいウェブサイト上に設定するための個人データの提供をまた最初からやり直すことを検討しなければなりません。これは、新しい企業への切替を検討している人々にとって、意欲を阻害するものとなります。

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.*
データ保護の改革：データポータビリティは、潜在的な顧客がサービスプロバイダ間で個人データを移動させることを容易にします。これにより、顧客が彼らの個人データを管理すると同時に、競争を促進し、市場における新規事業を奨励することができます。

What are the benefits for SMEs?
中小企業にとっての利益は何ですか？

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:

データ保護改革は、欧州の事業（中小企業も含む。）のため、コストと官僚的な面倒な手続を削減することにより経済成長を促進しています。（EU 加盟国数の）28 のルールの代わりに（EU 全体で）1 つのルールとするため、EU のデータ保護改革は中小企業が新しい市場に参入するのに役立つでしょう。多くの場合、データ管理者及びデータ処理者の義務は、事業の規模及び／又は処理されるデータの性質に合わせて調整されます。以下に例を挙げます。

- **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.
- 中小企業は、その主要な活動が大規模なデータ項目の定期的かつ体系的な監視を必要としない限り、又は人種や民族、宗教的信念等が明らかになるような特別な種類の個人データを処理する場合を除き、データ保護オフィサーを任命する必要はありません。更に、データ保護オフィサーは常勤の従業員である必要はなく、臨時の顧問でも良いため、多くの経費負担はかかりません。
- **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.
- 中小企業は、処理の実行が定期的である場合、又はデータ主体の権利と自由にリスクが生じない限り、処理活動の記録を保存する必要はありません。
- **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.
- 中小企業は、その違反の結果が彼らの権利と自由に高いリスクとならない限り、全てのデータ違反を個人に報告する義務はありません。

How will the new rules save money?
新しいルールはどのようにお金を節約しますか？

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**.
規則は唯一の汎欧州のデータ保護法として制定され、企業は（EU 加盟国数の）28 ではなく唯一つの法令に対応すれば良いことになります。新しいルールは凡そ年 23 億ユーロの利益をもたらすと見られます。

Example: Cutting costs
例：コスト削減

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.
あるチェーン店舗は、フランスに本社を置き、14 の他の EU 加盟国にフランチャイズ店舗を展開しています。各店舗は、顧客に関するデータを収集し、フランスの本社に転送して処理します。

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.*
現行のルールでは:フランスのデータ保護法は本社の処理に適用されますが、個々の店舗は、所在国の国内法に従いデータを処理したことを確認するため、各国のデータ保護機関に報告しなくてはなりません。これは、全支店の法令遵守を確実にするため、同社の本社が、現地の弁護士に相談する必要があるということです。全ての国の必要条件報告にかかる総費用は 12,000 ユーロを超える可能性があります。

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.*
データ保護改革では:データ保護法は EU 加盟国の 14 カ国全て、同じ – 1 つの EU の – 1 つの法になります。これによりフランチャイズ店舗について現地の法令遵守を確保するため現地の弁護士に相談する必要がなくなります。その結果、直接的なコスト削減と法的確実性が実現します。

How will the Data Protection Reform encourage innovation and use of big data?
データ保護改革は技術革新とビッグデータ利用をどのように促進するのでしょうか？

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.
一部の見積もりによると、欧州の市民の個人データの価値は、2020 年までに年間約 1 兆ユーロに増加する可能性があります。EU の新しい規則は、個人の基本的権利を保護しつつ、事業に柔軟性をもたらします。

'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.
「データ保護バイデザイン及びデータ保護バイデフォルト」は必須の原則になります。それは個人データの安全と保護のための新しい着想、方法、技術を革新し、開発する事業を奨励します。データ保護の影響評価と結合して使用されることで、企業は技術的および組織的ソリューションを創造する効果的な手段を得るでしょう。

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.
規則は個人データを保護するため、匿名化（不要な個人情報を特定できる情報の削除）、仮名化（個人識別可能な資料の人工的な識別子への置換）、暗号化（許可された人だけがそれを読むことができるようメッセージの符号化）といった技術を奨励します。これにより、匿名化または仮名化されたデータを使用して行われる「ビッグデータ」分析の活用が促進されます。

Example: Driverless cars
例：運転手不在の車

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.
運転手不在の自動車の技術は、個人データの交換を含む重要なデータの流動を要します。データ保護のルールは、革新的で進歩的なソリューションと連携しています。例えば、交通事故の場合、eCall 緊急通報システムを装備した車は、自動的に最寄りの緊急センターに連絡することができます。これは、EU のデータ保護の原則に沿った、実行可能で有効なソリューションの例です。

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.
新しいルールにより、eCall の機能はデータ保護の面でより簡単に、より単純に、より効率的になります。個人データが 1 つ又は複数の目的のために収集された場合、元の目的と相容れない方法で更なる処理をすべきではない、というのがデータ保護の原則です。これは、異なる目的のための処理を妨げたり、分析に「生データ」を使用することを制限したりするものではありません。

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.
新しい目的が元の目的と相容れないか否かの判断にあたり、公正か否かが鍵となる要素です。公正さは、個人のプライバシーへの影響(例えば、識別された人物についての特定の、導かれた決定)、個人データが新しい方法で使用されるだろうという理にかなった期待を個人が持つか否か、といった点を考慮します。

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.
よって運転手不要の車の場合、事故が多発するのはどこか、将来事故をどのように回避するかの分析に生データを利用することができます。交通渋滞減少のために、交通の流れの分析にも利用できます。

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.
企業は、たとえ分析の厳密な詳細がまだ分かっていなくとも、ビッグデータの利用可能性と利点を予期し、個人に通知することができます。企業はまた、将来の処理のためにデータを匿名化できるかどうかも検討すべきです。これにより、個人の権利を保護しながら、ビッグデータのための生データを保有することができます。

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.
新しいデータ保護ルールは、個人データの革新的な利用についての人々の取組みに影響を及ぼし得る、信頼の欠如を取り除く機会を企業にもたらします。明確で効果的な情報を個人に提供することは、分析とイノベーションに対する信頼を築くのに役立ちます。提供される情報は、データの処理方法ではなく、データ処理の目的です。

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.

革新的な製品とビッグデータ分析の明らかな複雑さは、義務付けられた人々の同意の取得に失敗することへの弁解ではありません。しかし、同意だけが処理の根拠ではありません。

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.
企業は、自由に、契約や法律、又は他の根拠が存在しない場合には、「利害関係の均衡」に基づき処理します。同意等、これらの「正式な必要条件」は、個人による個人データの制御の必要性と、全ての者に法的確実性を提供するとルールに規定されています。

How will the European Data Protection Board work?
欧州データ保護委員会はどのように機能しますか？

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.
現在、全ての欧州データ保護機関は、データ保護指令（指令 95/46/EC）第 29 条に基づき設置された「29 条作業部会」の下で会合を持っている。この作業部会は、EU 加盟各国のデータ保護機関、欧州データ保護監督者、委員会（投票権なし）の代表者で構成される欧州データ保護委員会（EDPB）に取って代わるものです。EDBP 議長は構成員の中から選ばれます。29 条作業部会と同様、EDPB は新しいデータ保護ルールが正しく適用されているかを監視し、関連する問題について欧州委員会に助言し、データ保護に関連する様々なトピックスに関する勧告と指導を行います。GDPR の新しい点は、EDPB が、各国のデータ保護機関の間で論争が避けられない場合にも拘束力のある決定を出し、EU 内のいたるところでデータ保護ルールの一貫した適用を促進することです。

What penalties will there be for businesses if they break the new data protection rules?
企業が新しいデータ保護ルールに違反した場合、どのような罰則が課せられますか？

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:
一般データ保護規則は、制裁金と課徴金を含む様々な新しいルールを遵守させるための手段を確立します。適切な罰金を決定する際は、各案件を注意深く評価し、以下の様々な要因が考慮されます。

- the gravity/ duration of the violation;
- 違反行為の重さ／継続期間
- the number of data subjects affected and level of damage suffered by them;
- 影響を受けるデータの件数と被る損害の程度
- the intentional character of the infringement;
- 違反の意図の性質
- any actions taken to mitigate the damage;
- 損害を軽減するためにとられた措置
- the degree of co-operation with the supervisory authority.
- 監督機関への協力の程度

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 not 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.
この規則は、守られなかった場合の罰金に 2 つの上限を設定しています。一つ目の上限は最高で 1000 万ユーロ、又は、事業の場合は全世界における年間売上の 2%までの罰金を課すものです。この一つ目の範囲の罰金は、例えば規則が必要とする影響評価を管理者が実施しない場合に適用されます。もっと高い罰金の上限は、最高で 2,000 万ユーロ、又は、全世界の年間売上の 4%となっています。例えば、規則の下保護されているデータ主体の権利を侵害する場合です。罰金は、個々の状況に応じて調整されます。

How does the GDPR protect personal data in case of cyberattacks?
サイバー攻撃においては、GDPR はどのように個人データを保護しますか？

- **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)

- GDPR には、個人データや処理に使用する装置への不正アクセス又は不正使用を妨げる等の、個人データの適切な安全性を保証する方法で個人データを処理する義務が含まれています。従って、管理者又は処理者は、個人データの処理にあるリスクを評価し、リスク軽減対策を実施する必要があります。(GDPR 第 32 条)
- **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)
- データ管理者は、過度に遅滞なく、データ違反についてデータ主体に通知する必要があります。この義務は、データ違反が生来の人の権利と自由に高いリスクをもたらし得る場合に、彼又は彼女が必要な予防措置を講じることを可能にするためのものです。(GDPR 第 33 条)
- **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)
- データ管理者はまた、個人データ違反が生来の人の権利と自由に危険をもたらす可能性が低いことを証明できる場合を除き、関連するデータ保護監督機関に通知しなくてはなりません。こういった通知は、過度に遅滞なく、可能な場合には一般にデータ管理者がそれに気付いて 72 時間以内に、出されなければなりません。(GDPR 第 34 条)
- **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.
- GDPR は、行政罰を課すための必要条件について明確に規定しています。データ保護機関は、例えばデータ違反のあった顧客やデータ保護機関に通知していない場合など、EU のルールを遵守しない企業に罰金を課すことができます。

How will the new rules work in practice?
新しいルールは実際にどのように機能しますか？

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.*

例：EU 加盟国の幾つかの拠点を持つ多国籍企業は、ヨーロッパ中にオンラインのナビゲーションとマッピングのシステムを持っています。このシステムは、全ての私有及び公共の建物の画像を収集し、個人の写真を撮影することもあります。

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.*
現在のルールでは：データ管理者に対するデータ保護規定は、各加盟国によって大きく異なります。ある加盟国ではこのサービス展開は大衆及び政治上の強い抗議を引き起こし、幾つかの側面では違法と見なされました。そこでその企業は、有力な DPA との交渉後にその加盟国に居住する個人に対して追加の保証と保護手段を提供しましたが、その企業は他の加盟国の個人に対して同じ追加保証の提供を約束することを拒否しました。現在、国境を越えて運営しているデータ管理者は、異なる、時には矛盾した義務を遵守するために、（法的助言や必要な書類等の準備に）時間と費用を費やさなくてはなりません。

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.*
新ルールでは：新しいルールは現行の一貫性のない各国法の寄せ集めに代わる、単一の汎ヨーロッパのデータ保護法を制定します。どの企業も－EU に拠点があるか否かに関わらず－EU でサービスを提供したければ、EU のデータ保護法を適用しなくてはなりません。

Example: *a small advertising company wants to expand its activities from France to Germany.*
例：小さな広告業社がフランスからドイツへ事業を拡大しようとしています。

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.*
現行のルールでは：そのデータ処理活動は、ドイツでは別のルールの対象となり、同社は新しい規制に対応しなくてはなりません。新規市場に参入するために法的助言を得て事業形態を調整する費用は途方もなく高くつきます。例えば、幾つかの加盟国はデータ処理の通知手数料を課しています。

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.*
新ルールでは:新しいデータ保護ルールは全ての通告義務とこれらに関する経費を不要とします。データ保護規則の目的は、越境取引の障害を取り去ることです。

What about the Data Protection Directive for the police and criminal justice sector?
警察や刑事司法部門のデータ保護指令についてはどうですか？

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.
警察の指令は、証人、被害者、容疑者など、刑事訴訟に関係する者の個人データ保護について保障します。また、加盟国の警察と司法機関の間の円滑な情報のやり取りを促進し、欧州におけるテロリズムや他の重大犯罪との闘いにおける協力を改善します。警察及び刑事司法分野の特有の性質を考慮しつつ、高水準のデータ保護を保障する包括的な枠組みを確立しています。

How does the Data Protection Directive for the police and criminal justice sector impact law enforcement operations?
警察及び刑事司法部門のデータ保護指令は法の執行にどのような影響を及ぼしますか？

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.
法の執行機関はより能率的かつ効果的にデータをやり取りすることができるようになります。データ保護に関する共通のルールは、(EU 加盟国数の)28 の異なる国の法律をより調和させ、法執行機関と司法機関が相互に効果的かつ迅速に協力できるようにします。完全に基本的権利憲章に沿い、法的に確かであるという条件の下、犯罪を防止するために必要な個人情報のやり取りを促進します。

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.
刑法執行機関はもはや、何の個人データかによって異なるデータ保護ルールを適用しなくても済み、時間と費用を節約できます。新しいルールは、国内の個人データ処理と国境を越えた個人データの移転の両方に適用されます。EU の全加盟国でより調和のとれた法律を持つことで、(複数の加盟国の)警察が協力しやすくなるでしょう。指令のルールは、刑法執行特有の必要性を考慮し、加盟国の様々な法的伝統を尊重します。

How does the Directive affect citizens?
指令はどのように市民に影響を及ぼしますか？

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.
個人のデータはより重く保護されます。データが刑法執行機関に利用される際、指令は市民の基本的なデータ保護の権利を守ります。全ての人の個人情報は、特定の目的だけのために合法的かつ公正に処理されるべきです。EU における全ての法執行処理は、個人に適切な保護措置を講じ、必要性、釣り合い、合法性の原則を遵守しなければなりません。独立した、国のデータ保護機関により確実に監督され、効果的な法的救済が提供されなくてはなりません。

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.
指令はまた、十分な水準のデータ保護を以て EU 外への刑法執行機関による個人データの移転が行われることを確実にするため、これらの移転に関する明確なルールを定めています。指令は、国内、欧州及び国際レベルでの個人データのやり取りに関する堅固なルールを提供します。

How does the Directive affect the work of criminal law enforcement?
指令は、刑法執行機関の業務にどのような影響を及ぼしますか？

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.

EU の全加盟国で同じ法律を持つことで、刑法執行機関が情報交換の際に協力しやすくなります。これにより、刑法執行がより能率的になり、より効果的な犯罪防止の状況を作り出します。

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.
これはまた、データ保護指令が、EU の自由、安全、正義の分野の発展の重要な要素と、EU の安全保障指針の構成ブロックと考えられる理由でもあります。指令は、以前警察及び司法機関によるデータ処理を規定していた Framework Decision 2008/977 / JHA に置き換わるものです。

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.
リスボン条約の発効と、特に新しい法的根拠の導入(第 16 条 TFEU)は、刑事上の案件に関する警察及び司法の協力の分野において、包括的なデータ保護の枠組みを確立させます。新しい枠組みは、個人データの国境を越えた処理と国内処理の両方に適用されます。

For more information
詳細はこちら

Statement/17/1436

MEMO/17/1441

Press contacts:
広報の連絡先:

- Christian WIGAND (+32 2 296 22 53)
- Melanie VOIN (+ 32 2 295 86 59)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email
一般の方のお問い合わせは:ヨーロッパ直接電話 00 800 67 89 10 11 又は電子メールで

- Last update: 20-02-2017 15:02:20 Version2.10.2-247
- 最終更新:2017 年 2 月 20 日 15 時 02 分 20 秒　第 2 版.10.2-247