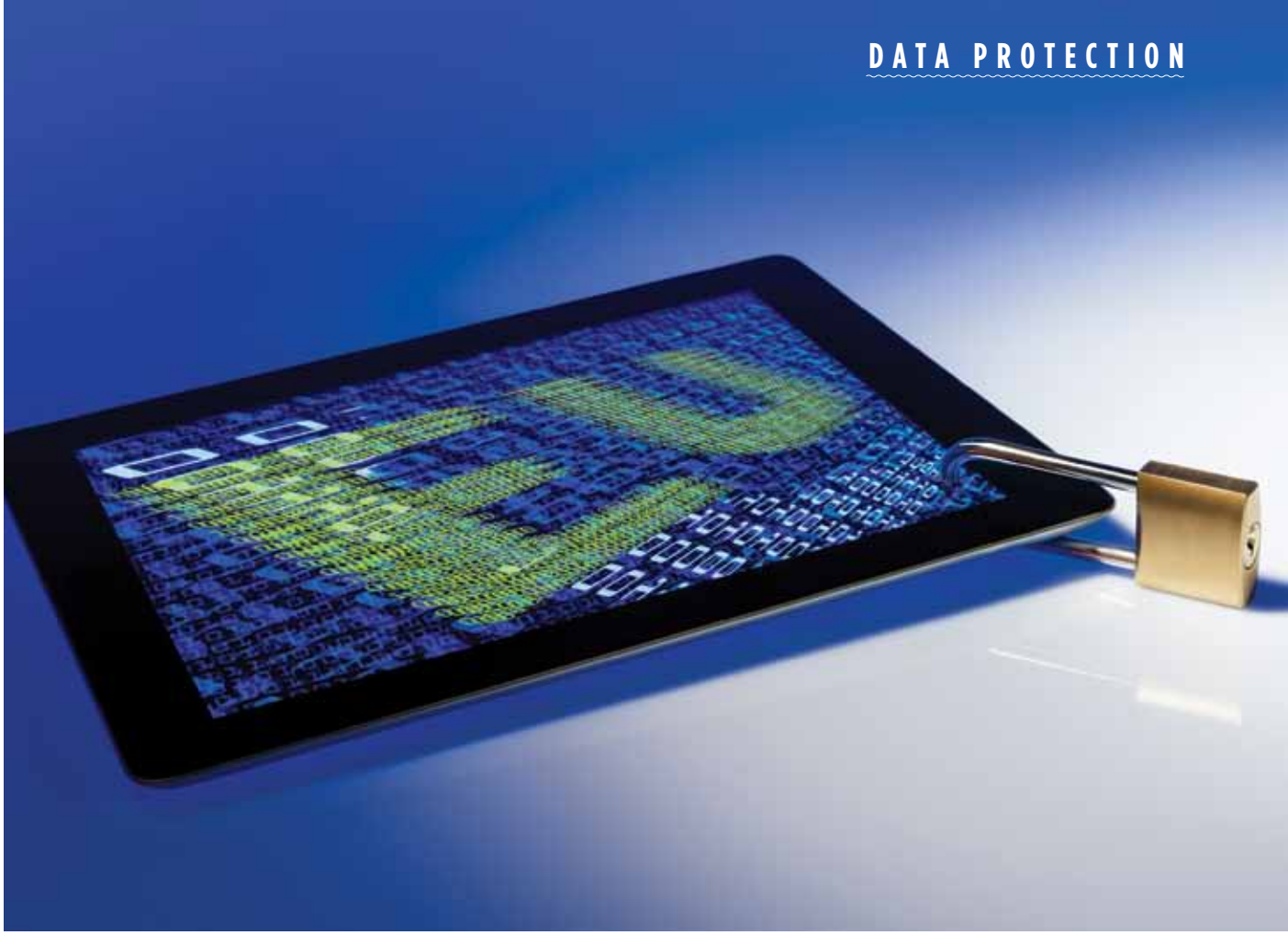

FINAL COUNTDOWN TO DATA PROTECTION

A long overdue reform in European data protection law has finally taken shape, as **MAURIZIO MENSI** explains

Data protection is undergoing a significant change across the European Union. A major review of the current European data protection framework was initiated in 2009 to further harmonise data protection legislation throughout Europe, as its current fragmentation is overly burdensome to market operators with cross-border activity. So the EU is in need of a new deal on data protection able to facilitate data flows, both in the EU and with its trading partners, and to guarantee the rights of freedom to individuals.

For this purpose, the European Commission's proposals for a comprehensive reform of the EU's 1995 Data Protection Directive[1] aim to strengthen privacy rights and boost Europe's digital economy by modernising the principles enshrined in the 1995 directive, bringing them into the digital age. The Commission's 25 January 2012 proposals include a policy communication setting out the Commission's objectives[2] and two legislative measures: a regulation setting out a general EU framework for data protection (GDPR), and a

directive on protecting personal data processed for the purpose of prevention, detection, investigation or prosecution of criminal offences and related judicial activities (EU Data Protection Directive).

Following the review carried out by the committees of the Parliament, on 12 March 2014 the European Parliament passed the compromise texts of the GDPR together with the police and criminal justice data protection directive. This rather swift approval was significantly influenced by 'Datagate', the mass interceptions scandal of the US National Security Agency's Prism programme, which emerged from revelations of analyst Edward Snowden in June 2013, relating to the collection of data on millions of phone users.

On 15 June 2015, ministers representing the member states at the EU Justice and Home Affairs Council agreed on a 'general approach' to the proposed GDPR.[3] The adoption of the approach carried with it authority for the presidency to lead negotiations with the Commission and the Parliament, setting the stage for achieving a compromise text to be adopted as the final regulation. The tri-party discussions kicked off in June with a view to adopting a text by the end of the year. The debate on the EU Data Protection Directive as well as GDPR by the Parliament and Council have been carried out in tandem, as the institutions have agreed on a flexible roadmap.

Finally, on 15 December 2015, representatives from the European Commission, the European Parliament, and member states reached an informal political agreement on the data protection package.[4]

COMPROMISE RESOLVING INSTITUTIONAL CONFLICTS

The GDPR sets out proportionate action and fines ranging from a warning or reprimand up to €20 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher, and sanctions are to be discretionary. A number of factors will be considered in setting the level of fines, including duration and gravity of the data breach, negligence and intention, and impact on users. Due regard should however be given to *"actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor"* (recital 118b).

The GDPR will establish a homogeneous set of rules on data protection in force across the EU uniformly. Recital 21 states: *"The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects as far as their behaviour takes places within the European Union."*

It follows that GDPR jurisdiction will extend outside the EU, as it applies to the offering of goods and services to, or the monitoring of, data subjects in the EU. Non-EU controllers that satisfy this jurisdictional connection will need to appoint an EU representative, "unless the processing it carries out is occasional" and "unlikely to result in a risk for the rights and freedoms" of individuals (recital 63).

Note that during negotiations, the Council of Ministers made important changes to the Commission's text and the present general approach differs markedly from the text adopted by the Commission in January 2012, as well as from the amendments to the Commission's text proposed by the European Parliament in its first reading in March 2014. A number of issues arise from disaccord among the institutions involved.

First, the GDPR brings forward a 'one-stop shop' for market operators and users, who will only have to deal with a single supervisory authority, simplifying cross-border operations and business. This apparatus is meant to guarantee consistency in the interpretation and enforcement of the regulation across the EU by supervisory authorities, significantly reducing costs and providing greater legal certainty in enforcement cases involving multiple data protection authorities. Nevertheless, the 'one-stop shop' provisions have been diluted by the Council, as in multi-jurisdictional breaches, where relevant supervisory authorities will need to be consulted and will be able to challenge the lead authority's assessment.

Moreover, in cases involving only one jurisdiction, the supervisory authority in that jurisdiction will preside over the matter, rather than the lead authority, as established by the 'one-stop shop' principle. This also implies a clarification of the competence of the supervisory authorities and the designation of a lead authority in cases of transnational processing. Data protection authorities should be ready to exercise their roles when the regulation enters into force, and determine proportionate and appropriate remedies and administrative sanctions on the basis of all relevant circumstances.

> **"The GDPR brings forward a 'one-stop shop' for market operators and users."**

Second, the GDPR mandates prior consent to be agreed before collecting and processing users' data. Data subjects must always be informed of their right to withdraw consent to the processing of their personal data. Also, "the data subject should be informed about the existence of profiling, and the consequences of such profiling" (recital 48). 'Profiling' is defined as any form of automated processing of personal data evaluating personal aspects as long as it produces legal effects concerning the data subject. The text approved on 15 December 2015 has defined more narrowly the nature of the informed consent, defining the boundaries of the quality of consent that data controllers must obtain to provide a legal basis for data processing, as it bears the adjective 'explicit'. On the contrary, the previous Council's draft required that consent "should be given unambiguously", which would have given data controllers more leeway in the subsequent use of data that was not contemplated at the time of

data collection. However, profiling in itself is not a source of concern. Instead, the absence of adequate information on the algorithmic mechanisms which prompt profiling and targeted advertising practices should be tackled though better transparency from data controllers, according to the general approach.

User profiling through possession of big data is central in some markets, such as online advertising, where there is the ability to create, through the technology of the internet, more accurate user profiles, which creates the ability to reach specific consumer types (by sending them targeted messages, with increasing levels of customisation) and to measure more precisely the effectiveness of advertising campaigns. In this perspective, strategic relevance is given to the collection of data about users, which constitute assets of crucial economic value, as they are likely to be included as part of the advertising industry. This calls for further neutrality and transparency on search-advertising platforms.

In this respect, Google has been accused of manipulating its organic search results to favour its own services. These allegations have often been accompanied by appeals for regulatory or antitrust intervention. They must nevertheless take into full account the two-sided nature of the search-advertising platform and the feedback effects that link the provision of organic search results to consumers, and the sale to businesses of advertising. The European Commission, in the framework of the digital single market strategy for Europe, launched in May 2015, plans to unveil a comprehensive assessment of the role of platforms and online intermediaries, which will cover issues such as transparency (eg. in search results), involving paid-for links and/or advertisements.

As for breach notification, the GDPR dictates that supervisory authorities and affected individuals must be notified of violations that are likely to jeopardise the rights and freedoms of individuals, with notice to supervisory authorities "without undue delay and, where feasible, not later than 72 hours". This approach differs from that pursued by the Commission in stipulating compliance obligations that must be fulfilled by all data controllers, which is less risk-tailored. The Commission initially suggested that notification of data security breaches be made within a period of no longer than 24 hours of the data controller becoming aware of the violation.

Another notable feature of the proposed regulation is the explicit enshrining of the right to be forgotten, which is now accepted as a European general principle, following the landmark case by the European Court of Justice (ECJ). On 13 May 2014, the ECJ held that, by searching systematically for information published on the internet, indexing websites, recording and making it available, the operator of a search engine is 'processing' personal data within the meaning of Article 2(b) of Directive 95/46/EC (see the Google Spain case).[5] Following its earlier decision,[6] the Court confirmed that, even when the information collected by the operator of a search engine had already been published elsewhere by others, the search engine's related activities still must be classified as processing under the directive.

The decision required Google to consider individuals' requests to eliminate links that they say impinge on their privacy. This provision would give anyone the right "to obtain from the controller the erasure of personal data [...] without undue delay" (the 'data controller' is essentially the entity that makes decisions about how and for what purpose data is processed). The GDPR explicitly acknowledges to the data subject the right to obtain from the controller the erasure of personal data without undue delay (see article 17).

REFORM OF THE E-PRIVACY DIRECTIVE

The year 2015 was undoubtedly one of great change. The new Commission, headed by Jean-Claude Juncker, ambitiously set the goal "to take, within the first six months of [his] mandate, ambitious legislative steps towards a connected digital single market". Even though the Connected Continent package was partially unsuccessful due to strong conflicts between the Council and Parliament (because its scope was curtailed to roaming and net neutrality), the Commission's digital single market (DSM) strategy is nevertheless a programme of welcome initiatives, ambitious in aim, scope and implementation timing.

> **The rationale of the GDPR has been supported and reinforced by the DSM strategy.**

The rationale of the GDPR has been supported and reinforced by the DSM strategy, which irons out 16 targeted actions to be delivered by the end of 2016. One of the actions calls for a reform of Directive 2002/58/EC (the e-privacy directive).[7] Privacy is a matter of great importance to EU citizens, as two-thirds are worried about not having full control over the information they provide online.[8] Indeed, adoption of the GDPR, which will replace Directive 95/46/EC, will have consequences also for the e-privacy directive, which is *lex specialis* (governing law) for the electronic communications sector.

In this vein, the DSM strategy calls for a reassessment of the e-privacy directive, particularly since most of the articles of the current directive exclusively apply to providers of electronic communications services – that is, traditional telecoms companies – and does not include in its scope information society service providers using the internet to provide communication services.

ECJ STANCE ON THE DATA RETENTION DIRECTIVE

European institutions must also adhere to the ECJ's judgment that declared the Data Retention Directive,[9] which related to telecoms data, invalid in 2014. The ECJ established that, although the retained data did not comprise the content of the communications, data could *"allow very precise conclusions to be drawn concerning the private lives of*

the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them".

In other words, the ECJ held that the directive restricted subscribers' privacy because *"the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance"*. The directive did not ensure a retention period "limited to what [was] strictly necessary" as it instituted a minimum retention period of six months without distinguishing between different sorts of data or different types of users, and a retention period of between six months and two years without requiring any "determination [that the] period must be based on objective criteria".

For those reasons, the ECJ declared the data retention directive invalid, holding that it did not satisfy the principle of proportionality, and should have assured more safeguards to protect the fundamental rights of freedom of expression, respect for privacy, and protection of personal data, guaranteed by the Charter of Fundamental Rights of the EU.

As president of the European Parliament, Martin Schulz, remarked in response to the ECJ's ruling, any new proposal must *"respect in every detail the guarantees laid down in the Charter of Fundamental Rights [...], enshrin[ing] a high level of data protection – which is all the more essential in the digital age – thus avoiding disproportionate interferences with the private lives of citizens"*. Hence European institutions cannot ignore the ECJ's decision regarding personal data and privacy. In particular, the proposal for the EU data protection directive must be in conformity with the ECJ's ruling.[10] By the same token, the ECJ and the national courts have to take into account the Charter of Fundamental Rights in judging cases where EU law is at stake.

Interestingly, the advisory Article 29 data protection working party[11] also called on member states to gauge the consequences of the ECJ pronouncement on national data protection laws, remarking that *"there is no bulk retention of all kinds of data and that, instead, data are subject to appropriate differentiation, limitation or exception"*.

Increasing reliance on the possession of user data is a prominent feature of today's information society. Data is an extremely valuable asset in a number of sectors, for instance in online search advertising. It enables players in the search advertising industry to move swiftly into neighbouring markets, such as contextual, display, email and general, non-search advertising. The tendency towards convergence of these different formats of advertising, owing to the development of behavioural advertising and the trend to mix and match diverse advertising strategies by the major players in the industry, has been remarked on by the European Commission during the course of investigations into both Google/DoubleClick and Microsoft/Yahoo.[12]

At the same time, data possession generates barriers to entry by conferring to the incumbent advantages that cannot be replicated by potential entrants. In particular, other entities engaged in offering internet search advertising will barely be able to match the quality of the results offered by a dominant firm, which can strengthen its position by simultaneously playing in multiple, parallel markets where it can acquire, verify, test and obtain additional specification of the information gained in the normal search advertising context.

As a consequence, data-driven markets are likely to be much less precisely defined around a certain product or service, and much more on a participant's ability to use those data across different types of activity. Thus a crucial element in defining these markets is describing the scope to which the privacy policy specified in the terms of use of the website (or search engine) permits utilisation of the information received from the user in other contexts, as well as the provision of another service by the same company ('intra-company versatility') and for other companies to provide another or even the same service ('inter-company portability').

"Increasing reliance on the possession of user data is a prominent feature of today's information society."

INVALIDATION OF THE COMMISSION'S US SAFE HARBOUR AGREEMENT

Edward Snowden's revelations of mass surveillance on EU citizens impacted on the so-called safe harbour scheme, which includes a series of principles concerning the protection of personal data to which US undertakings may subscribe voluntarily.[13] Specifically, on 6 October 2015, the ECJ declared invalid[14] the European Commission's transatlantic data protection agreement from the year 2000, holding it does not adequately protect consumers. Indeed, EU privacy law forbids the movement of its citizens' data outside of the EU, unless it is transferred to a location which is deemed to have 'adequate' privacy protections in line with those of the EU.

The safe harbour agreement had permitted companies to self-certify that they would protect EU citizens' data when transferred and stored within US data centres, developing a single standard for consumer privacy and data storage in both the US and Europe, without the need to ask for consent, or to enter into bilateral agreements.

In fact, even the European Commission had previously expressed doubts on the appropriateness of the safe harbour scheme. In a communication in November 2013 it acknowledged the growing concern among some data protection authorities in the EU about data transfers under the scheme, and pointed out that *"some member states' data protection authorities have criticised the very general formulation of the principles and the high reliance on self-certification and self-regulation. Similar concerns have been raised by*

industry, referring to distortions of competition due to a lack of enforcement."[15]

In its landmark ruling, the ECJ specified that the European Commission did not have the competence to restrict national supervisory authorities' powers in protecting the personal data of their citizens. Interestingly, the ruling came less than a week after the ECJ judgment in the Weltimmo case,[16] in which it held that international companies should abide by the data protection legislation of the jurisdictions in which they operate (the case concerned a property website company registered in Slovakia but was 'operating' in Hungary).

Following the invalidation of the safe harbour agreement, American companies, including internet behemoths such as Google, Facebook, Apple and Microsoft, must strive for striking 'model contract clauses' to authorise the transfer of data outside of Europe, thus guaranteeing an adequate level of protection in line with EU rules. In this vein, it is likely that big US companies will be building EU-based data centres to handle data for EU citizens.

Nonetheless, it should be noted that the EU is currently negotiating with the US for an upgraded safe harbour to meet the ECJ's concerns, while ensuring certainty and clarity.

COUNCIL OF EUROPE MODERNISATION OF CONVENTION NO. 108

In parallel with the legislation initiative of the Commission, the Council of Europe (CoE) in March 2012 presented its proposals for updating the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108).[17] In October 2011, the parliamentary assembly of the CoE made a recommendation backing the reinforcement and globalisation of Convention 108.[18] In November 2012, the CoE consultative committee adopted its final proposals for modernisation, and submitted them to the Committee of Ministers for adoption.[19] Eventually, the ad hoc committee on data protection of the CoE approved on 3 December 2014, after discussions and amendments, the modernisation proposals of the convention. A draft amending protocol is to be arranged on this basis and transmitted to the Committee of Ministers for examination and adoption.[20]

Although the EU and CoE share the same concerns on data protection, their approaches differ. The convention, which serves as a sort of universal standard, is less prescriptive and more focused on human rights (see its preamble).[21] But its coherence and compatibility with the European regulatory framework remain key objectives.

THE WAY FORWARD

Negotiations to reform EU rules on data protection are in the final stage. On 17 December 2015, the EU Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE) voted on the informal agreement on the data protection package.[22] The reform package's final texts will be voted on and formally adopted by the European Parliament and Council later in 2016, probably in March or April. From then there will be a two year timescale for its entry into force.

Against this backdrop, the DSM strategy will play a crucial role. The challenge is in dealing with highly technical matters while being confronted by strong political stances that are not always conducive to facilitating the path towards implementation. The DSM strategy is supposed to deliver different actions by the end of 2016, with the support of the Parliament and Council.

> **A balance should be struck between hyper-regulation and a dangerous lack of data protection.**

Because of these potential conflicts, a balance should be struck between the risk of a race to hyper-regulation – which would threaten to stifle the dynamic digital market – and a dangerous lack of comprehensive data protection within the European Union.

MAURIZIO MENSI *is professor of economic law at the National School of Administration (SNA) and of information and communications law at LUISS Guido Carli University, Rome. He is a member of the Rome Bar and has been admitted to practice before the highest court of Italy. Mensi focuses on communications and media, IT, privacy and data protection, copyright, cyberlaw and regulation of public utilities.*

REFERENCES **1** Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. **2** Safeguarding privacy in a connected world: A European data protection framework for the 21st century. bit.ly/1IlhkYe **3** Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – Preparation of a general approach. bit.ly/1ShoM8T **4** Agreement on Commission's EU data protection reform will boost digital single market. EC press release, 15 December 2015. bit.ly/1J9ZUdt **5** Google Spain – judgement of 13 May 2014. bit.ly/1MKoqFS **6** Satakunnan Markkinapörssi and Satamedia – judgement of 16 December 2008. bit.ly/1LEUqHq **7** Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector. See the Commission's DSM strategy, pillar II, action 12. **8** Eurobarometer survey on data protection, June 2015. bit.ly/1LPx1Ho **9** Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, amending Directive 2002/58/EC. **10** Proposal for a directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25 January 2012. bit.ly/1Tj7acV **11** The Article 29 working party comprises a representative from the data protection authority of each EU member state, the European Data Protection Supervisor and the European Commission, as set out in Article 29 of Directive 95/46/EC. **12** See Case COMP/M.4731 Google/Double Click; Case COMP/M.5727 Microsoft /Yahoo Search Business. **13** Commission decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. **14** Judgment in Case C-362/14. The Court of Justice declares that the Commission's US Safe Harbour decision is invalid. 6 October 2015. bit.ly/1FUc1iu **15** Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU. bit.ly/19VRFqN **16** Judgment in Case C-230/14. Weltimmo s.r.o. vs Nemzeti Adatvédelmi és Információszabadság Hatóság. 1 October 2015. bit.ly/1VrPhIG **17** Convention for the protection of individuals with regard to automatic processing of personal data, adopted by the Council of Europe in 1981. ETS No. 10. **18** Council of Europe parliamentary assembly, recommendation 1984 (2011): The protection of privacy and personal data on the internet and online media. **19** Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data (T-PD). Modernisation of Convention 108: Final document. Strasbourg, 29 November 2012. **20** Ad hoc committee on data protection. 3rd meeting. 1-3 December 2014. bit.ly/1sumsTF **21** "Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing [...] recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples." Preamble, Convention No. 108. **22** New EU rules on data protection put the citizen back in the driving seat. European Parliament press release, 17 December 2015. bit.ly/1JECFse