Most of its elements have serious implications for HR. Designed to protect the Facebook generation from postings they made of youthful indiscretions, her proposed ‘right to be forgotten’ could play havoc with businesses’ employment records. A new army of ‘compliance’ officers, charged with checking that the new rules are being followed, would be imposed on every business with significant operations in Europe. This paper examines these and other threats posed by the draft legislation and suggests that consideration should be given to ways of treating employment data differently from other forms of data.

On January 25, 2012 the European Commission published its proposal for a General Data Protection Regulation (GDPR) as the centerpiece of a broad and comprehensive overhaul of data protection law.

The GDPR impacts many aspects of data protection, from long-established issues relating to the provision of goods and services, to newer concerns around social networking sites. However, proposals in this area also have serious implications for HR with regard to the gathering and transfer of employee personal data. These can be particularly tricky for businesses based outside the EU, especially US multinationals.

Its authors talk about strengthening the internal market dimension, ensuring a high level of data protection for individuals, and promoting legal certainty, clarity and consistency for business while building trust in online services. This suggests a balanced approach, recognising on the one hand the way in which technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities and, on the other, how freely individuals make personal information available publicly and globally.

In fact, the proposals as they stand move mainly in one direction: more duties imposed on the ‘data controller’ and ‘data processor’ regarding the management of data – in other words, on business; more power to the ‘data subject’ – the employee or customer – to review and limit the information held on them and how it is used; and much tougher policing – by data commissioners at EU and national level with the power to impose draconian fines, and by the activities of a vast new army of independent ‘data officers’ who are to be employed by every organisation with over 250 employees.

Essentially, this amounts to an attempt by the EU authorities to impose globally a much more restrictive regime on data management than applies anywhere in the United States and to reverse the powerful tide of openness that the new social media have generated.
Why a ‘Regulation’?

Why do they want to introduce a Regulation rather than a Directive? Most EU law is brought in through Directives, requiring that EU Member State governments within a certain time frame, typically two or three years, pass their own national legislation implementing the requirements of a Directive. This process leaves Member States with a certain amount of flexibility as to the exact rules to be adopted and provides considerable scope for them to adapt the requirements to fit their jurisdiction. Frequently this involves providing greater protection than the minimum required by the directive. But not always: national laws implementing and particularly enforcing a Directive can vary considerably between member states, and some are relatively weak.

In the case of the current Data Protection Directive, introduced in 1995, the Commission discovered that many had not properly implemented it at all. Rules across Member States differ widely, as do the resources and the powers of the national authorities responsible for data protection. Indeed, some member states have only recently got round to implementing the existing Directive.

That, to the Commission, is unacceptable. In this new digital environment, the Commission argues, data protection still remains a fundamental right enshrined in Article 8 of the Charter of Fundamental Rights of the European Union, as well as in Article 16(1) of the later Treaty on the Functioning of the European Union (TFEU), and needs to be protected accordingly. Individuals have the right to enjoy effective control over their personal information.

They also point out that, under the Directive, businesses have to deal with up to 27 different national laws and requirements, which causes uncertainty, unnecessary costs and administrative burdens and discourages them from expanding their operations across borders.

Power to the EU Commission

By contrast, a Regulation offers a more powerful form of EU law and will become effective and enforceable as law in all Member States simultaneously two years after it is adopted. It will supersede member states national laws without any further legislative action within the Member States. The European Commission (EC) has now concluded that the EU needs a more comprehensive and coherent policy on the fundamental right to personal data protection and to achieve that goal a “Regulation” rather than a “Directive” is required.

While the uniformity across the EU promised by the Regulation is attractive to business, the power it gives to the Commission is a cause for concern. A great deal of care is required in the drafting and formulation of any set of legislative provisions if they are to become acceptable and workable in every Member State. Detailed knowledge of local practice and an awareness of the commercial impact of change are not skills which the Commission staff are normally called upon to exercise or even possess. Nor will their involvement in the development and application of policy cease once a Regulation is agreed. Throughout the text of the GDPR there are worrying references to “implementing acts” and “delegated acts”. These “acts” will give the Commission the power to specify detail about how a particular article of the GDPR should work. How the Commission might use these powers needs careful scrutiny now, long before they win any right to do so.
Main measures and their impact on HR

The Regulation that has been tabled and which would replace the current Directive covers a lot of ground. Many of its provisions are not directly targeted on data about employees or the management of employees. But experience of the existing Directive has demonstrated how wide-ranging the impact of Data Protection rules can be. For example, in the UK, where Government normally seeks to implement EU labor laws with a ‘light touch’, their impact on the employment relationship has been substantial. The Employment Practices Code produced by the UK’s Information Commissioner under the Directive runs to 91 pages and has detailed guidance on every aspect of the employment relationship, from recruitment and selection through employment records and monitoring at work to information about workers health.

- Consent: The GDPR changes (the regulation states “clarifies”) the conditions for consent to be valid for the processing of data. Consent must be ‘explicit’ and it must be specific both in terms of the data being collected and the purposes for which that data is to be used and disclosed. Commonly, businesses seek to obtain a wide-ranging consent through the use of paragraphs in the contract of employment documents. Under the Regulations, the emphasis is on obtaining free and informed consent; if such consent is contained in a document dealing with other issues, such as an employment agreement, the personal data transfer consent part must be clearly distinguishable – by highlighting the passage or putting it in a separate document – or it will be ineffective. Moreover, Article 7 provides that “Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.” It might be argued that incorporation into an employment contract as the employment relationship is formed is an imbalance and that therefore consent in a separate document entered into after the employment relationship is established will always be necessary.

- Personal Data: The GDPR reaffirms the current broad interpretation of what constitutes “personal data” under EU law to include any information relating to living individuals. This underscores the difference between the EU’s requirements and data protection laws in other jurisdictions, including the US, where there is no national (as opposed to some individual state) laws equivalent to those implemented by Directive 95/46/EU. Any country that fails to share this broad definition has little chance of being judged to have equivalent protection for any transfers of personal data from within the EU.

- Access: Individuals will continue to have rights to access their information held by a data controller, including their employer. As many companies have already experienced, this can cause difficulties where individuals use such “subject access request” rights to circumvent litigation disclosure and/or, more often, to go on a “fishing expedition” for evidence on which to base claims against their employer. The Commission takes a very negative view of companies charging for the provision of such data. Although there may still be some scope at national level to allow such charges, there must be concerns that allowing individual employees to make complex and time-consuming data requests could lead to abuse, including their mass use as a costly lever against the employer in labor disputes.
• Right To Be Forgotten: This new right would require data controllers to delete personal data relating to a data subject where the individual withdraws consent, objects to that controller’s processing of their information, or where their personal data is no longer needed. The obvious target of this provision is social media, and the Commission’s concern that people should be able to delete information about themselves that they no longer want to appear on these sites. In an employment context, however, it raises a number of concerns, notably about the retention of data on someone who has left the company’s employment. That person may want the data deleted; but it may prove vital later, if for example, he or she subsequently brings a case for discrimination against the business, or if the Revenue want to see records. How is HR to know if they can resist an employee or ex-employee exercising such a right?

• Data Protection Officers: This is possibly the single most significant proposal for employers. All public authorities and large private companies (i.e., with 250 or more staff) will be required to appoint a data protection officer (DPO) for a minimum term of two years which term can be renewed. Their function is simply to ensure data protection compliance. They will have protection from dismissal during their term(s) of office, comparable to that applying to Works Council members in some EU countries now. They are to be appointed on the basis of their professional qualities and, in particular, expert knowledge of data protection law and practice. Essentially, the Regulation aims to establish a new profession and to oblige employers to pay for thousands of these people to act as data protection police within their business. This places the issue of data protection in an almost unique position in the workplace.

• Accountability: Data controllers – in other words, every business – would be required to adopt policies and appropriate measures to ensure, and be able to demonstrate, compliance with the GDPR. This is a new principle of “accountability” and will need a prescriptive control framework to be in place to ensure data protection compliance. It is not clear how this will be expected to work, but the implication is that the business will have to be able to demonstrate not only that they have appropriate and up-to-date policies, but that people are kept informed about any changes to them and, potentially, that all relevant employees have been trained to apply them.

• Breach Notification: the Regulation wants to see this become a very rapid process. Companies will be required to notify the national Data Protection Regulator of any personal data breach without undue delay: not later than 24 hours after having becoming aware of it wherever feasible. In addition, the data subject(s) must also be notified of the breach after notification has been given to the national regulator. This new "24 hour" rule is a significant change and again its target may be social media, but it also means businesses will be required to “go public” with bad news very fast with the associated reputational risk. In an employment context, this could have serious labor relations consequences. For example, if names of people who may be at risk of redundancy were to be sent by error to an outside agency even before consultation had started, the employer could be left in a very exposed position –having to tell employees that this information had been released to outsiders before there has been any opportunity to begin due process.
Fines: Businesses that are found to have breached the new data protection rules would be liable to potentially crippling fines: up to €1 million or up to 2% of their global annual turnover (i.e. revenue!)

Supra-national Data Protection regulation: Data controllers and data processors will no longer have to deal with data regulatory bodies in each EU country where they operate. Rather they will principally be regulated by the data protection regulator in the EU country where they have their "main establishment". That is defined as the establishment in the EU where the main decisions as to the purposes, conditions and means of the processing of personal data are taken. However, individual employees can refer to the data protection regulator in the country of their own employment, even when their data is processed by a company based outside the EU.

Data Portability: Individuals will have the right to transmit information which is processed electronically to another electronic system. This is aimed at digital media, and also at digital vaults and any products which store customer information. However, it might also cover portability of data about an employee that the employee wants to send elsewhere, perhaps to a new or prospective employer, or even to his union.

Responsibility for Data Processors: Data subjects will have the right to claim compensation from data processors and data processors will need to implement appropriate security measures to protect personal data. This may be aimed at IT vendors and service providers, and the data they hold on customers, or client businesses personnel, but it could have wider effect. Processors will assume direct legal risk under the new rules.

Responding to the EU Commission’s plans

It is 17 years since the EU first addressed this topic in the Data Protection Directive (95/46/EC). That Directive caught many businesses napping, and wrought havoc for US headquartered multinationals with EU operations when they belatedly realized that the transfer of personal data from within the EU to the USA was going to be a major issue. This was because the US was not – and still is not – on the EU list of approved countries considered to have a sufficient level of data protection law to meet Europe’s standards. On that occasion, US and other non-European multinational firms and their governments were far too slow to understand what the EU was doing and to take action accordingly.

True, much diplomatic and business lobbying was subsequently deployed in the late 1990’s on the issue of transferring personal data to the US. By then, however, the EU legislation was already firmly in place. Eventually a few routes were carved out to get round the problem: the creation of the US-EU Safe Harbor Program administered by the FTC; the facility for developing Binding Corporate Rules within multinational corporations; and also the use of EU approved model contract clauses. These are all potentially impacted by the new proposals and this remains a perpetual cause for concern for major businesses seeking to manage change with an increasingly mobile global workforce. True, the use of Binding Corporate Rules would win clearer recognition under the proposed Regulation; but it remains unlikely that the EU will determine that the US is a jurisdiction that provides an adequate level of data protection to permit the free transfer of personal data – indeed, the Regulation may well empower the Commission to
establish yet more demanding rules in this respect. Meanwhile, the majority of the world’s businesses, including those on whose growth future economic prosperity mainly depends, and who are not based in Europe, may well contest Europe’s right to set the rules for all countries in this critical area.

There are some points in the new proposals with which employers will see as sensible – though they may query whether the EU rather than a body with a much wider membership like the OECD or UN is the appropriate body to determine such issues with a global impact. But now that the GDPR has been published, businesses affected by it from both within the EU and other countries, particularly those multinationals headquartered in the US, need to provide valuable input before any final adoption by Europe’s legislators in a year or two’s time.

US businesses and their representative organizations accordingly need both to become actively involved in the current debate, so as to ensure that the application of any EU Regulation in this area makes good business sense and is practically feasible, and to alert their Governments to the global impact of this proposed Regulation. They need to draw particular attention to the potential effects on HR practices of the GDPR as a matter of urgency. Otherwise these important, practical, business issues will be lost in the hype and controversy over how far the GDPR affects Facebook, Linked In, Google and the rest of the social media. Corporate America should not again delay until Europe has already imposed a law, the thrust and location of which they may question and the practical effects of which could damage their business.

The full text of the proposed Regulation can be viewed here: