The new EU Data Protection Regulation: what will the impact be on the life sciences industry?

William Long, *Anna Pavlou* and *Jessica Walch* explain which areas of the European Commission's proposed regulation on data protection will need to be ironed out if the final text is to be balanced and appropriate.

The EU Data Protection Regulation proposed by the European Commission in January will – if adopted in its current form – require pharmaceutical and medical device companies to adopt a new approach to data processing and data protection[1].

The ability to collect, analyse and transfer personal data, in particular health data used in clinical trials, adverse event reporting and medical research, is critical both to the life sciences industry and to society, more generally, to ensure progress in medical science and safety. Accordingly, life sciences companies need to consider carefully the proposed regulation on data protection.

The commission's proposals, overall, constitute an improvement with regard to recognising that a balanced approach to data protection is required in areas such as pharmacovigilance and medical research. However, the practical impact of many of its provisions is, as yet, unclear.

The data protection requirements proposed also require close attention because the new regime will introduce a more aggressive enforcement approach, with fines of up to 2% of a company's annual worldwide turnover. In addition, data protection authorities will be able to impose a temporary or definitive ban on processing personal data, enter premises and suspend data flows to a recipient located in a non-EU member state or to an international organisation. Moreover, any organisation that aims to protect the data protection rights of individuals, such as consumer organisations, will have the option of making complaints to data protection authorities and bringing actions on behalf of individuals (ie data subjects) for non-compliance with the proposed regulation.

The proposed regulation on data protection will be subject to much discussion and possible revision as it progresses through the EU legislative process – this will probably last until 2014. Due to the impact of the proposals on use of health data, the potential increase in compliance costs and greater enforcement actions, companies should ensure they become involved in these discussions to ensure that the final text is balanced and appropriate. Once adopted, the new regulation will replace the current EU Data Protection Directive (Directive 95/46/EC)[2].

The new regime will introduce a more aggressive enforcement approach

Impact on pharmacovigilance

Under the new EU pharmacovigilance legislation – Directive 2010/84/EU[3] and Regulation (EU) No 1235/2010[4] – pharmaceutical companies have strict obligations to report adverse events related to a medicinal substance or product. In particular, all serious suspected adverse reactions in the EU and third countries that are reported to the marketing authorisation holder must be submitted to the EudraVigilance database, managed by the European Medicines Agency, within 15 days. Similarly, all non-serious suspected adverse reactions that occur in the EU will have to be submitted electronically to the same database within 90 days[5]. Such obligations involve the processing of personal data and present particular data protection issues for pharmaceutical companies.

Pursuant to the Volume 9A Rules Governing Medicinal Products in the European Union, individual adverse event case reports must contain:

- an identifiable healthcare professional reporter;
- an identifiable patient who can be identified by initials, patient number, date of birth, age or age group or sex; and
- details on at least one suspected active substance/medicinal product[6].

The proposed regulation on data protection maintains the current prohibition on processing personal data concerning health or sex life except where certain exemptions apply. The most relevant exemptions include the following instances:

- the data subject has given consent;
- the processing is necessary to protect the vital interests of the data subject;
- the processing of health data is necessary for health purposes; or
- the processing is necessary for historical, statistical or scientific research.

However, the proposed regulation specifically allows health data to be processed for reasons of public interest in the area of public health, including to ensure high standards of quality and safety for medicinal products or medical devices[7]. Does this include adverse event reporting? Such broad reference in the proposals to the processing of health data in the area of public health, including to ensure quality and safety, would seem to cover pharmacovigilance activities. However, the life

sciences industry should consider the pros and cons of having a specific reference to pharmacovigilance activities to avoid any doubt.

Also relevant to pharmacovigilance is the exact scope of personal data. For example, does a patient identification number amount to personal data[8]? This question was also examined by the European Data Protection Supervisor in two opinions[9,10]. For the EDPS, a key factor in determining whether data is anonymous is traceability. According to the EDPS, data are considered anonymous only if it is impossible to identify (or retrace) the person to whom the data relate[11].

However, the view of member states can differ particularly on whether key-coded data, such as a patient identification number, amounts to personal data. For example, it is understood that in Belgium and Sweden, pseudonymised data (such as key-coded data) can still amount to personal data if any third party (such as the physician) has a key that can be used to re-identify an individual. In other member states such as Denmark, Finland, France, Italy and Spain, the position on whether pseudonymised data is personal data appears to be ambiguous[12]. However, the authorities in these countries tend to agree with the Belgian approach whereby, in principle, all data that can be linked to an individual is considered to be personal data, even if processed by someone who cannot make that link[13]. Lack of consistency between member states on such a fundamental question has been of particular concern for pharmaceutical companies, regulators and individual data subjects.

The proposed regulation clarifies the position and now explicitly states that personal data relating to health should include a number or symbol assigned to an individual to uniquely identify the individual for health purposes, which presumably would include a patient identification number[14].

As for anonymous data, the proposals provide that the principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. However, this leaves open the question of whether an individual can be identified from a combination of different pieces of information even where a patient identification number is not used, such as initials and date of birth. In this case, the proposed regulation applies a similar test to the one that exists under the Data Protection Directive that account should be taken of all the "means likely reasonably to be used" either by the data controller or by any other person to identify the individual[15].

Another key aspect of data protection requirements and pharmacovigilance – as identified by the EDPS – is that only health personal data that is "absolutely necessary" should be collected and included in an individual case safety report (ICSR). Such a requirement is reflected in the proposed regulation, which provides that data controllers must implement mechanisms for ensuring that, by default, only the personal data that is necessary for each specific purpose is processed and is not collected or retained beyond the minimum necessary for those purposes[16]. This requirement of data minimisation means that life sciences companies will in practice need to carry out a data protection impact assessment to ensure that only the minimum data necessary for the purpose of pharmacovigilance are being processed[17].

Consent will continue to be an important legal justification for processing personal data

Impact on clinical trials

New obligations on data processors

Clinical trials involve numerous parties, each performing different roles and having different responsibilities. These parties include sponsors, investigators, clinical research organisations (CROs) and many other parties such as laboratories and statisticians.

Under the Data Protection Directive, entities involved in a clinical trial are defined as either data controllers or data processors. Importantly, only data controllers are directly subject to the requirements laid down in the directive. Consequently, pharmaceutical companies acting as the sponsor of a clinical trial and the trial centres that carry out the trial in complete autonomy but in compliance with the sponsor's guidelines are considered to act as joint data controllers. In contrast, a CRO is normally considered to be a data processor, although it is ultimately a question of fact to be determined on a case by case basis[18].

The proposed regulation on data protection keeps the current distinction between data controllers and data processors. However, the scope of many of its requirements now applies to both data controllers and data processors, such as the obligation to maintain detailed documentation of the processing operations including details of the purposes, types of personal data, recipients, international transfers and time limits for retention of personal data. Similarly, both data controllers and data processors are now required to implement appropriate security measures and, where there are over 250 employees, appoint a data protection officer for a term of at least two years. Consideration will need to be given to the consequences of this change in regulatory responsibility for data processors, which may require an examination of existing contracts with service providers involved in clinical trials such as CROs.

Data protection impact assessment

The proposed regulation introduces an administrative simplification by abolishing the current notification requirements that exists in some member states for sponsors to register the processing of personal data as part of clinical trials with the national data protection authority where the trial is performed. However, there is now a proposed requirement that a data protection impact assessment be carried out by the data controller or the data processor where the processing operations present specific risks, such as the processing of health data. In such a case, the proposed regulation requires data controllers to seek the views of data subjects or their representatives on the intended processing and consult with the data protection authority regarding the data protection impact assessment.

The requirement to conduct data protection impact assessments and prior consultation could significantly impact life sciences companies and service providers involved in clinical trials, and other activities involving health data. In practice, this may require conducting a detailed review of such activities and taking measures to ensure that, through use of privacy by design, compliance with the new data protection requirements can be demonstrated to data protection authorities and data subjects.

New requirements for consent

Obtaining patient consent is a key aspect of clinical trials and other activities of life sciences companies. Under the proposed regulation, consent will continue to be an important legal justification for processing personal data, including health data. However, the proposals require that such consent must be given explicitly, with the data controller having the legal burden of proving that the data subject has given valid consent. In addition, where the consent is to be provided in a written declaration, the requirement to give consent must distinctly appear in the document – and be kept separate from consent to be given in the context of other matters.

The proposed regulation also 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 data controller". The application of such a condition to clinical trials could be problematic as, arguably, there is an inherent imbalance between the position of the individual patient and the life sciences

company. In this event, the controller will have to find legitimate reasons other than the data subject's consent to justify the processing of personal health data. Life sciences companies should look to obtain clarification on this issue as the proposed regulation progresses through the legislative process.

The proposals also provide further guidance in the event that a patient withdraws their consent, stating that such withdrawal shall not affect the lawfulness of processing the data that has been previously provided. It should be clarified whether this means that personal data can continue to be used in a clinical trial as from the date on which the data subject's consent was withdrawn.

Impact on medical research

Conducting secondary research

Medical research is a key activity of the life sciences industry. However, there is uncertainty as to the ability to carry out scientific research in compliance with the Data Protection Directive. In particular, it appears to be unnecessary and impractical to apply the full data protection requirements under the directive to key-coded research data where the recipient has no access to the key and thus cannot identify the individual. Similarly, consent requirements may impede medical research because the original consent does not necessarily cover secondary research, such as further examination of the disease or examination of the unanticipated secondary benefits of a drug. However, it is not always possible to anticipate all secondary research purposes at the time of the initial research.

While the proposed regulation does not specifically exclude key-coded data from its scope, it does permit health data to be processed for scientific research if:

- the scientific purpose of the research cannot be fulfilled by processing data that does not permit identification of the data subject; and
- the data enabling the attribution of information to an identified data subject is kept separately from the other information. This scientific research exemption appears specifically designed to give greater flexibility to the life sciences industry to process key-coded research data.

However, there still appears some confusion over whether research data processed for an initial research purpose can be processed subsequently for a secondary research purpose. The proposed regulation provides that processing of personal data should only be allowed where the processing is "compatible" with those purposes for which the data have been initially collected, in particular where the processing is necessary for scientific research purposes[19]. Where the secondary purpose is not compatible with the initial purpose, the proposed regulation further provides that consent should be obtained from the individual or another legitimate ground for processing should be used[20]. Further clarification is required as to whether the scientific research exemption, referred to above, means that personal health data can be used for a secondary research purpose that is not compatible with the initial research purpose provided that the data is key coded.

The proposed regulation on data protection introduces new rights that will have a very significant impact on social media both for users and providers of social media

In addition, the proposed regulation provides that bodies conducting scientific research may publish, or otherwise publicly disclose, personal data if: (i) the data subject has given consent; (ii) the publication of the personal data is necessary to present research findings or to facilitate research provided the rights of the data subject do not override these interests; or (iii) the data subject has made the data public[21]. It is unclear how pharmaceutical companies and other life sciences bodies should determine whether the fundamental data protection rights of individuals outweigh the publication of the research findings. In practice, this presumably means that a data protection impact assessment should be required to determine whether the research overrides the interests of the data subjects.

Impact on social media

Social media is increasingly being used by individuals, patients, healthcare professionals and life sciences companies as a means of interacting with communities and to obtain awareness of diseases and products. For example, vast numbers of individuals now willingly provide their personal data in interactions as part of patient social media communities. The data collected on those websites in addition to being shared with other users could be sold to the social media provider's partners, such as companies that are developing or selling pharmaceutical products or medical devices to patients.

The proposed regulation on data protection introduces new rights that will have a very significant impact on social media both for users and providers of social media. In particular, the proposals introduce a new right to be forgotten, under which individuals can require that a data controller erases their personal data where the data are no longer necessary, the individual withdraws consent or objects to the processing or where the personal data are not processed in compliance with the proposed regulation. In addition, where the data controller has made the data public, it must take all reasonable steps to inform third parties that a data subject requests that they erase any links to or copies of the personal data. The proposed right to be forgotten presents a number of challenges for all companies involved in social media. In particular, it is questionable whether it is technically possible to erase all personal data on the internet. While it is possible to delete a social media account, it is difficult to delete data that is out of the user's control. Where the personal data has been accessed by others on a social media application there is no means of knowing who has had access and how they have used the data. In a digital age of user generated content, it is highly questionable whether it is possible to stop the spread of personal data across the internet.

The proposed regulation provides an exemption from the obligation to erase personal data mentioned above. This exemption applies where the retention of the personal data is necessary for historical, statistical and scientific research purposes. This necessity test means that each life sciences company as a data controller will need to make its own subjective determination of whether it is necessary to retain the personal data for scientific research purposes. This is a concern because any right which may allow individuals to erase their data could have a significant impact on the validity of scientific findings in clinical trials, epidemiological studies and medical research. Such a right also appears contradictory to the acknowledgement in the proposed regulation that withdrawal of consent shall not affect the lawfulness of data processing based on the consent previously given by an individual.

A further issue for medical research in relation to social media is the exemption under the proposed regulation that bodies conducting historical, statistical or scientific research may publish personal data if the data subject has made the data public. Does this mean that individuals who have made their personal data "public" by disclosing such data on Facebook and other social media forums may legitimately have their personal data published for the purpose of scientific research?

Achieving the right balance

It is clear that the proposed regulation on data protection will have an important impact on life sciences companies and will require a new approach to data protection. To examine the precise impact further clarity is required on a

number of its principles and provisions. However, this clarity may be a long time coming, as one of the main concerns with the proposals is that a large number of its provisions will need to be supplemented by what is called a "delegated act" or an "implementing act" setting out further details and requirements. The technical standards and requirements in these acts will not be adopted by the commission until the proposed regulation is adopted and will not be open to general public consultation. Consequently, some important details of a number of provisions in the proposed regulation will only become clear once those necessary acts are adopted. The legislative financial statement to the proposed regulation estimates that the commission may handle three implementing measures a year, while the process could take up to 24 months – this means it could take 15 years to implement all 45 delegated acts and implementing measures in the proposed regulation.

Life sciences companies should ensure that they fully consider the proposals and become involved in discussions on the regulation as it moves through the legislative process. Getting the right balance, in an ever more digitally globalised world, between strengthening data protection rights for individuals and stimulating progress and innovation of medical science and research is a critical issue both for the life sciences industry and society.

References

1. *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), 25 January 2012, http://bit.ly/xNQK8P*
2. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ, 23 November 1995, L 281, 31-50*
3. *Directive 2010/84/EU amending, as regards pharmacovigilance, Directive 2001/83/EC, OJ, 31 December 2010, L 348, 74–99, http://bit.ly/pqehjA*
4. *Regulation (EU) No 1235/2010 amending Regulation (EC) No 726/2004 and Regulation (EC) No 1394/2007, OJ, 31 December 2010, L 348, 1–16, http://bit.ly/pqehjA*
5. *Directive 2001/83/EC of 6 November 2001, Article 107, OJ L 311, 28 November 2001, 67-128*
6. *Guidelines on Pharmacovigilance for Medicinal Products for Human Use, Volume 9A of The Rules Governing Medicinal Products in the European Union, September 2008, http://bit.ly/yy1IQA*
7. *Article 81 of the proposed regulation on data protection.*
8. *Opinion of the working party on the concept of personal data, adopted on 20 June 2007, 4/2007, WP 136, available, http://bit.ly/x2bL0l*
9. *Opinion of the EDPS, 2009/C 229/04, 23 September 2009, OJ C 229, 19, http://bit.ly/zcWsN2*
10. *Opinion of the EDPS, Case 2008-402, 7 September 2009, http://bit.ly/xRubCE*
11. *Opinion of the EDPS, 2009/C 229/04, OJ, C 229, 23 September 2009, 12*
12. *McCullagh K, A study of data protection: harmonisation or confusion?, 21st BILETA Conference: Globalisation and Harmonisation in Technology Law, April 2006, Malta*
13. *Ibid*
14. *See Ref 1, Recital 26*
15. *See Ref 1, Recital 23*
16. *See Ref 1, Article 23*
17. *See Ref 1, Article 33*
18. *Opinion 1/2010 on the concepts of "controller" and "processor" – WP 169 adopted on 16 February 2010, http://bit.ly/fiXdkz*
19. *See Ref 1, Recital 40 and Article 6(4)*
20. *See Ref 1, Article 6(4)*
21. *See Ref 1, Article 83*

William Long is counsel in Sidley Austin LLP, London, UK. **Anna Pavlou** and **Jessica Walch** are both associates in Sidley Austin LLP, Brussels, Belgium. Website: www.sidley.com. Email: wlong@sidley.com. The views expressed in this article are personal to the authors and do not reflect the view of Sidley Austin or any of its clients.