PHARMAnetwork®
strategy, organization, finance, outsourcing
magazine

N° 30 - 2016

Raising the bar on Biopharma Manufacturing Quality

New EU general data protection regulation: what changes does it bring, including for the life sciences sector?

By Cécile Théard-Jallu and Jean-Marie Job

On December 15, 2015, following the final round of a "trilogue" between the European Parliament, the Council and the Commission, the three of them **reached an agreement in principle on a compromise text for the new EU General Data Protection Regulation ("GDPR").**[1] The current regime is primarily governed by Directive 95/46/EC, which used to respond to the twin objectives of protecting the fundamental right to personal data protection and guaranteeing the free movement of such data between Member States".[2] However, substantial divergence had arisen in the way the 1995 rules were implemented and enforced across the European Union and they progressively appeared to be no longer adapted to an increasingly digitalized economy. Therefore, starting in 2009, the Commission has launched a series of public consultations on data protection and a dialogue process with EU national data protection authorities as well as other major stakeholders, to explore options for a new data protection regime that would be more consistent and comprehensive across all EU Member States.[3]

Following years of negotiations, the GDPR was finally released, while still needing to receive formal adoption by the EU before its official publication, expected to occur in the course of 2016.

All this being said, the current version is already worth the analysis by EU and non EU operators if they want to anticipate the soon to come impacts of the GDPR on their day-to-day activities. This is all the more necessary as it comes in a context of increased tensions between the EU and the US around the Safe Harbor issue: the invalidation of the 2000 Safe Harbor Agreement by the European Union Court of Justice on October 6, 2015 in the "Schrems" case[4] causes EU-US personal data flows to no longer be automatically authorized from a EU law standpoint based on the assumption that US data[5] rules would not be sufficiently protective of European subjects' personal data ; despite huge lobbying actions by major US big data players urging the EU to accept data processing rules in force in the US, EU and US authorities currently have meet great difficulties in reaching an agreement on a Safe Harbor 2. A "EU-US Data Privacy Shield" agreement was finally adopted on February 2, 2016 and will deserve deep scrutiny in view of the strategic issues at stake at a global level.

Beyond this new agreement, the GDPR will soon establish a general regulatory scheme for the protection of EU subjects' personal data being processed by EU and non EU operators. Adopted in the form of a Regulation (and no longer a Directive as was formerly the case with the Directive 95/46/CE that it will have for its effect to repeal), this regime will directly apply in all Member States' laws and will come into force within two years as from the date of its official publication *i.e.*, in 2018 in principle.

The GDPR is designed, on the one hand, to strengthen EU citizens' right to personal data protection, which is enshrined in the December 7, 2000 EU Charter as a fundamental right, and on the other hand, to stimulate growth and innovation.[6] The objective of fostering economic growth is first achieved by easing administrative burdens for companies, such as the repealing of the mandatory notification to supervisory authorities and the creation of a one-stop-shop regime.[7] As a result, the harmonized scheme is expected to allow savings for EU companies of approximately €2.3 billion per year.[8] Second, the higher degree of personal data protection embodied in the proposed Regulation is designed to restore consumers' trust in online services and to "fulfil the potential of the digital economy", which in turn serves to "foster innovation" and encourage the "competitiveness of EU industries".[9]

As far as your company is concerned, the GDPR now establishes a uniform and harmonized framework for the processing of personal data, which will be applicable to all companies, regardless of their place of establishment and whether the processing takes place within the EU or not. Moreover, as a result of its expanded territorial scope, data controllers and processors established outside the EU now falls within the perimeter of the GDPR, if they offer goods or services to, or if they monitor the behavior of, EU residents.

Health data occupies a particular place in the new regime with, among others, a new definition of the notion of health personal data, the inclusion of genetic data in the category of sensitive data or a specific chapter being devoted to data

processing in the framework of researches. However, the GDPR shall not bring any substantial change to life science actors' day to day personal data processing practices compared to already existing mechanisms, in addition to the more general changes brought by the GDPR.

Subject of course to any last minute modification that may always pop up before it is finally enacted, let's focus on **the key provisions of the GDPR and what will be this limited impact on the life sciences sector.**

I. What are the main changes brought by the GDPR from a general standpoint?

1. Strengthening the Protection of Citizens' Personal Data

In its communication regarding the safeguarding of privacy in a connected world (25/01/2012), the European Commission had explained that the aim of its proposed regulation is *"to strengthen rights, to give people* ***efficient and operational means*** *to make sure they are fully informed about what happens to their personal data and to enable them to* **exercise their rights more effectively."**[10]

The GDPR confirms this announcement by reiterating already existing fundamental principles and introducing new mechanisms:

(i) The **fundamental rights** governing personal data processing **remain the same**: *e.g.*, right to access data, to have one's data rectified, erased, right to data security, lawfulness of data processing, trustworthiness, transparency etc.....

(ii) **Data subject's consent** is paramount, especially for sensitive categories of personal data, for which consent still need to be "explicit"[11] (Articles 7 & 9). Data controllers are now required to show that the data subject has given his/her consent to the processing of their personal data in a free, specific, informed and *"unambiguous"* way, *"either by a statement or by a clear affirmative action"* (Article 4).

(iii) **Parental consent** shall be given where the processing concerns personal data of a child below 16 years old; The text leaves the option open to Member States to lower such age limit to 13 years old (Article 8).

(iv) The **information right** is reinforced: individuals shall be provided with a higher level of information about how their data is being handled; Moreover, this information should be made available in a clear, concise, transparent, understandable and easily accessible form (Articles 12, 14, 15).[12]

(v) The **"right to be forgotten"** is clarified: in a number of situations, a person from whom data has been collected, may withdraw his/her consent to have his/her data processed in the future; for instance when the data is no longer necessary in relation to the purposes for which it was collected, or when the data has been unlawfully processed, or upon erasure of the data being required by a legal obligation by which the data controller is bound... etc.; more globally speaking, provided that there is no other legitimate ground to retain it, the data will be deleted if so requested by the data subject (Article 17). [13]

(vi) A **right to data portability** is created with a view to facilitating the transfer of one individual's personal data; this right entitles a person, whose data has been collected under a standard form, to freely transfer the stored data from one data controller to another "without hindrance" (Article 18).

(vii) In the case of **non-authorized access to personal data**, data controllers will be under the obligation to notify such data breaches to both (a) national data protection authorities (DPA) without undue delay, and where feasible within 72 hours having become aware of it, and (b) to the individual concerned by the breach (Article 31 & 32).

2. Alleviating the administrative burdens for businesses... to a certain extent

The objective of the agreement is to create a harmonized legal environment for data protection as a way to stimulate economic growth and foster innovation, which is accomplished "by cutting costs and red tape for European companies." Companies will no longer need to navigate among the divergent national data protection regimes and will now only be bound to report to one single supervisory authority ("one stop shop").

(i) **Prior authorization from the supervisory authorities is no longer required on the part of data controllers for the data** processing they conduct, except for the collection and processing of sensitive personal data. The DPAs, under the supervision of European authorities, will determine what data qualifies as "sensitive data."

(ii) **Data processors** shall implement **"appropriate and technical measures"** to ensure and demonstrate that their companies' internal data collection process complies with the provisions of the GDPR (including privacy by design by which technological tools used to process data shall themselves allow for the compliance with data protection rules). Data controllers will need to implement appropriate data protection policies. The adherence to approved codes of conduct or to an approved certification mechanism can serve as proof of compliance with this obligation (Article 22). This is the so called "accountability" obligation by which data controllers shall demonstrate that they comply with the new data protection regime.

(iii) Under certain circumstances, companies processing or collecting personal data are bound **to appoint a data**

protection officer (DPO): where (i) the processing is carried out by a public authority; or if (ii) the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or if (iii) its core activities consist in processing sensitive data on a large scale. Controllers or processors shall otherwise not be bound to appoint a DPO unless required to do so by their national law (Article 35).

(iv) Companies are required to conduct a prior **impact assessment** of the forecasted personal data processing operations where the contemplated processing is likely to result in a high risk for the rights and freedoms of individuals. The supervisory authority establishes and publishes a list of the types of processing operations for which an impact assessment is required (Article 33). If the impact assessment reveals that such processing would create such a risk, then the data controller must consult the relevant supervisory authority, which may advise the data controller on the matter or impose certain enforcement measures, such as for instance further auditing measures, corrections or restrictions to the scope or modalities of the processing.... (Articles 34 & 53). After a few months of implementation, it will be interesting to study the real financial impact of this new mechanism as we may not be so certain that this will effectively alleviate operators' financial burden contrary to what the GDPR's looks for...

3. Transfer of Data to non EU Countries

GDPR's provisions on data transfer to non-EU Member States deserve particular attention in view of the Safe harbor agreement's invalidation by the **ECJ** on October 6, 2015:

(i) **No specific authorization for data transfer is required** provided that the European Commission is satisfied that recipient third country (of the transfer) offers sufficient and adequate level of protection. The Commission makes this decision based on a series of criteria such as inter alia the country's compliance with the rule of law, the way it preserves human rights and fundamental freedoms, its national data protection rules and security measures, or the existence and effective functioning of an independent supervisory authority in that country (Article 41).

(ii) If the Commission is not satisfied with the adequacy of the level of protection, the transfer will not require authorization if the data controller or processor provides **appropriate safeguards,** such as a legally binding and enforceable instrument between public authorities, binding corporate rules approved by the competent DPA (Article 43) or standard data protection clauses adopted or approved by the Commission or DPAs, or an approved code of conduct which must be legally binding and enforceable (Article 42). In any event, enforceable data subject rights and effective legal remedies for data subjects shall be available.

(iii) In any event, transfer of data to a non-EU party is possible provided that the data subject **explicitly consented** to the transfer, after having been **informed of the possible risks** attached to such transfer in the absence of an adequate level of protection and appropriate safeguards, or when such transfer is necessary to the performance of a contract between the controller and the data subject or the implementation of pre-contractual measures taken at the subject's request, or is justified by important reasons of public interest or answers the need to establish exercise or defend legal claims (Article 44).

4. Strengthening of independent supervisory authorities' powers

(i) **Data Protection Authorities** (DPAs) will be endowed with a series of powers, including **corrective powers** or the power to impose high **pecuniary sanctions** in case of infringements. More precisely, the DPAs will be able to impose fines that may reach an amount of up to €20,000 or in case of an undertaking, up to 4% of the company's total worldwide annual turnover of the preceding fiscal year, whichever is higher. They shall take into account factors such as the nature, gravity and duration of the infringement, or the intentional or negligent character of the infringement, or the action taken by the controller to mitigate damages (Article 79).

(ii) The GDPR creates an independent European Data Protection Board (EDPB), which will be composed of the head of one DPA for each Member State and of the European Data Protection Supervisory (Article 64). The EDPB contributes to the functioning of the "consistency mechanism" around the GDPR (Articles 58-63).

II. What is the GDPR's specific impact for life sciences actors?

Building on the sensitive personal data provisions of the 1995 Directive, Article 9.1 of the GDPR keeps the **general prohibition** on the processing of sensitive data which now include genetic data in addition to data relating to health (which was already mentioned in the past).

As in the past, Article 9.2 lists some **exceptions** to this prohibition:

- Paragraph (a), when the data subject gives his or her **explicit consent** to the processing of his or her personal data. **However, Member States and the Union may now decide that the general prohibition may not be lifted by the data subject. This could create inconsistencies between the various EU Member States despite the GDPR's objective of harmonization.**

- Under paragraphs (b) and (c), the prohibition does not apply where the processing is necessary for the purposes of carrying out the obligations and specific rights of the controller or of the data subject in the **field of employment and social security**, or where the processing is necessary to protect the vital interests of the data subject;
- Paragraph 2(h) provides for specific rules with respect to the processing of health data. It indicates the **purposes for which health data may be processed**, which include preventive or occupational medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care services. Sensitive personal data may be processed for those purposes when it is processed by or under the responsibility of a professional who is subject to an obligation of professional secrecy under Union or Member State laws (Paragraph 4);
- Moreover, the processing of those sensitive data may be permitted if it is necessary for **reasons of public interest** in the area of public health or social protection (Paragraph (hb), or for **scientific research purposes** (Paragraph (i)); from the standpoint of pharmaceutical laboratories and their partners, this legal basis will certainly be the most useful tool to accompany their personal data processing projects; indeed, they generally process and control health data in the course of their research and development activities. Note that the "public interest" justification is generally the one used to validly conduct health personal data processing in the course of pharmacovigilance activities.

Here are the main changes specific to the processing of health data, that companies operating in the field of life sciences should pay attention to in addition to other changes brought by the GDPR:

(i) Article 4 of the GDPR offers an express definition of what is meant by **"data concerning health"** ***i.e.***: *"data related to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status."*

(ii) The sensitive personal data regime now also covers **genetic data**, which is defined as *"all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from the analysis of a biological sample from the individual in question"* (article 4(11)). This novelty is of importance as genetic data is more and more used in the pharmaceutical sector, including for the development and registration of both medicinal products and biomarkers, namely, but not only, within the scope of personalized medicine projects.

(iii) Article 83 of the GDPR allows the European Union or EU Member States to provide for **derogation with respect to the processing of personal data for scientific research purposes,** as long as those derogations comply with certain conditions and safeguards for the rights and freedoms of data subjects.

(iv) In addition to the provisions of the GDPR, life sciences companies (in particular health care companies) **must be wary of the national law of each Member State** in which they plan to process personal health or genetic data. Under the GDPR, "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or health data" (Article 9.2 Paragraph 5).[15] Again, this may be a source of inconsistency between the laws of EU Member States despite the global harmonization intent behind the GDPR.

Although not specifically related to the life sciences sector, the global changes brought by the GDPR as synthetized in Section I above, may substantially impact the actors of this sector. In particular:

a. **The criteria for data subject's consent collection have been reinforced**, especially for sensitive categories of personal data such as health data. Although already implemented under some national laws, the obligation to obtain a free, explicit, specific, informed and "unambiguous" consent on the part of the patients will now be globally all the stronger for sponsors organizing clinical trials.

b. Data controllers, who are no longer required to notify national DPAs of their data processing projects, must however conduct an **impact assessment**, before processing **certain categories of data** (Article 33). Most notably, the GDPR now requires a prior impact assessment in the case of sensitive personal data, where the processing of such data is performed for the purpose of taking decisions concerning data subjects on a large scale. Health data is directly impacted by this change and one may not be so sure that this will alleviate the costs borne by pharmaceutical companies and their partners when processing personal data despite the financial savings announced as one of the GDPR's goals as mentioned in our introduction above.

c. The **right to be forgotten** may negatively affect the findings of clinical trials or medical researches since individuals may ask for their data to be erased. Not to mention the data that now circulates through social media, for instance web sites dedicated to healthcare professionals, and which it may be hard to recuperate should a data subject decide to exercise this right. ■

Notes

1. http://europa.eu/rapid/press-release_IP-15-6321_en.htm.
2. COM(2012) 11 final. 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).
3. COM(2012) 9 final. Communication from the Commission to the European Parliament, the Council, the European and Social Committee and the Committee of the regions, Safeguarding Privacy in a Connected World : A European Data Protection Framework for the 21st Century.
4. http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN.
5. Under the 2000 Safe Harbor regime, US companies had the possibility to self-certify to a given data protection charter allowing them to import personal data from the EU even though the US were not deemed a country with an adequate level of protection compared to EU standards. This self-certification is no longer possible pursuant to the 2000 regime following the "Schrems" decision of October 6, 2015.
6. Reform of EU data protection rules (http://ec.europa.eu/justice/data-protection/reform/index_en.htm).
7. Agreement on Commission's EU data protection reform will boost Digital Single Market, Press Release from the European Commission, 15 Dec. 2015 (http://europa.eu/rapid/press-release_IP-15-6321_en.htm).
8. Reform of EU data protection rules (http://ec.europa.eu/justice/data-protection/reform/index_en.htm).
9. COM(2012) 9 final. Communication from the Commission to the European Parliament, the Council, the European and Social Committee and the Committee of the regions, Safeguarding Privacy in a Connected World : A European Data Protection Framework for the 21st Century.
10. COM(2012) 9 final. Communication from the Commission to the European Parliament, the Council, the European and Social Committee and the Committee of the regions, Safeguarding Privacy in a Connected World : A European Data Protection Framework for the 21st Century.
11. GDPR, p.3.
12. Agreement on Commission's EU data protection reform will boost Digital Single Market, Press Release from the European Commission, 15 Dec. 2015 (http://europa.eu/rapid/press-release_IP-15-6321_en.htm).
13. Ibid.
14. Agreement on Commission's EU data protection reform will boost Digital Single Market, Press Release from the European Commission, 15 Dec. 2015 (http://europa.eu/rapid/press-release_IP-15-6321_en.htm).
15. GDPR, p.9.

About the authors

Cécile Théard-Jallu - Partner Attorney
ctheardjallu@dgfla.com

Cécile Théard-Jallu has developed in-depth expertise as an attorney in private practice representing multinational corporations, including major US and European firms and organizations in the R&D and healthcare sectors. Cecile focuses primarily on complex transactions including IT, R&D and consortiums, technology transfers, licensing deals and other technological change related projects. She assists clients with their responses to project offers in the R&D and innovation sector in the context of public funding.

She worked for over one year as an attorney in private practice in Covington & Buriling LLP, a leading law firm in Washington DC, and was also seconded to a global player in the medical equipment sector. She regularly lectures on innovation and research law and is a member of the Internal Bar Association in the Healthcare practice.

Jean-Marie Job - Partner Attorney
jmjob@dgfla.com

Jean-Marie Job has highly specialised experience in the pharmaceutical industry combined with in-depth expertise in the field of health law (pharmaceuticals and biotechnology sectors), new technologies and data-privacy.

He is also involved in issues related to the management of personal and commercial data. For fifteen years, he practiced in the legal department of a major pharmaceutical group before joining de Gaulle Fleurance & Associés in 2001.

He is an honorary member of the Association of Pharmaceutical Industry Lawyers and regularly lectures on health law. He is also recognized by the health department of the Data Protection Authority (CNIL) as a trusted specialist.