Cloud computing for s-Health and the data protection challenge

Getting ready for the General Data Protection Regulation

Rossana Ducato
Faculty of Law, University of Trento
Trento, Italy
rossana.ducato@unitn.it

***Abstract*—The recently approved General Data Protection Regulation (GDPR) will change deeply the European privacy framework. Despite the aim of updating the legislative provisions to the challenges of the information society, the GDPR leaves open serious questions and shortcomings, especially in the context of cloud computing for s-health. The purpose of the paper is twofold: after having outlined the major innovations of the new GDPR for ensuring data protection in cloud environments, paying particular attention to the processing in the healthcare sector, the main unresolved issues will be critically addressed.**

Keywords—cloud computing; s-health; e-health; privacy; electronic health records; data protection; security; GDPR

I. INTRODUCTION

In the last years, cloud computing has become an efficient technological solution for the storage, processing and use of data on remotely computers accessible via web, thanks to which the users "can command almost unlimited computing power on demand, that they do not have to make major capital investments to fulfill their needs and that they can get to their data from anywhere with an internet connection"[1]. This potential makes the cloud particularly interesting for applications in many different sectors and businesses. The healthcare field is no exception in this regard, as cloud promises costs savings and more effective, scalable and interoperable IT services [2]. Furthermore, cloud-based applications allow a concrete implementation of the so-called smart-health (s-health), which visionary goal is the "provision of health services by using the context-aware network and sensing infrastructure of smart cities" [3]. In other words, s-health aims to integrate ubiquitous computing and ambient intelligence to the concept of P4-Medicine (i.e. a predictive, personalized, preventive and participatory medicine supported by smart technologies and analytical tools, where the patient plays a central role) [4-5], creating an infrastructure for connecting all the different nodes, which generate health data (electronic health records, patient summaries, m-Health applications, wearable sensors, etc.) and provide healthcare assistance (hospitals, first aid services, general practitioners, etc.), in order to offer high-quality and personalized medicine while increasing the efficiency of the national healthcare systems. In this regard, cloud computing is the necessary technological precondition for allowing the integration of such a great variety of sources of information and devices, and the use of advanced data mining methods for analyzing health data [6].

However, despite its potential benefits, cloud computing is not widespread adopted. One of the major barriers is related to the lack of a specific regulatory framework for cloud services [7]. Applicable laws exist, but they are rather fragmented and regulate only sectorial aspects (data protection, security, consumer protection, contract rules for the terms of service, liability of the Internet service provider, etc.). Indeed, cloud computing poses a number of issues, especially in the domain of data protection law [8-11]: the architecture itself of such a technology, the complex chain of actors involved, the quantity and variety of the information collected, the transnational flow of data, the consequences of breaches may result in a lack of control over personal data and an insufficient transparency with respect to cloud providers' (CPs) processing [8]. Furthermore, cloud computing highlights obsolescence of the current legislation and the difficulties in ensuring compliance with it. In an effort to both update the privacy framework to the challenges of the information society and harmonize the provisions of the Member States, the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, hereinafter "GDPR") has been recently adopted. Such an act will replace Directive 95/46/EC and it will be self-executing. Even if the GDPR does not expressly mention cloud computing, in accordance with the principle of technological neutrality, its provisions apply and some of them seem to be designed with cloud in mind. GDPR will enter into force in the spring of 2018, so both CPs and SMEs or PAs looking for cloud services must start preparing a switchover to the new rules in order to avoid costly bottlenecks.

The aim of the paper is twofold: after having outlined the major innovations of the new GDPR for ensuring data protection in cloud environments, paying particular attention to the processing in the healthcare sector, the main privacy unresolved issues will be critically presented.

This work has been financially supported by Cardioline Spa.

978-1-5090-1846-8/16/$31.00 ©2016 IEEE

II. How the GDPR shall affect cloud computing

The GDPR is going to introduce several innovative provisions and will have a significant impact also on the cloud-based data processing. In this regard, one of the most relevant new developments brought in by the Regulation is the broadening of the scope of application of data protection rules. Directive 95/46/EC was in fact essentially controller-centered: its obligations were built around the figure of the data controller, i.e. the subject which determines the purposes and means of the processing; meanwhile, the GDPR now expressly takes into account the role played by the data processor, i.e. the person or body that processes personal data on behalf of the controller. This has an evident impact on cloud, because according to Art. 29 Working Party (WP29) CPs (IaaS, PaaS and just pure SaaS) are considered data processors [8].

For the first time, with the GDPR data processors are direct subjects to specific duties: Art. 28, GDPR states that processors have to offer sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of GDPR and ensure the protection of the rights of the data subject. This provision is a precondition for choosing a CP, since the GDPR introduces new rights for data subjects and, as consequence, new duties for controllers that need to entrust a processor who ensures the adequate compliance with novel principles, such as the right to data portability, the right to be forgotten, the right to data access or the privacy-by-default. Adherence of a processor to an approved code of conduct or an approved certification mechanism as referred to in Art. 42 may be used as an element by which to demonstrate compliance with GDPR requirements. However, in the case of cloud computing the latest version of the "Data Protection Code of Conduct for Cloud Service Providers", drafted by the Cloud Select Industry Group, a working group composed of representatives of industry, did not receive the favorable opinion of WP29 [12].

Secondly, in line with Opinion 5/2012 of the WP29, processors cannot outsource their activity, engaging another processor, without prior specific or general written authorization of the controller. This provision takes into account the complexity that cloud processes may reach, ensuring both transparency and accountability, since it allows a processor to appoint another processor, as long as the controller agrees. Furthermore, the GDPR harmonizes a point, which was differently implemented in the legislation of Member States: while, countries like France, UK, Germany, Austria, Luxembourg, Portugal and The Netherlands provided the possibility of the processor to outsource its activity, the Italian law enables only the data controller to appoint a processor [13]. The GDPR also establishes that controllers and processors shall enter into a binding contract, setting out the main aspects of the processing, such as its subject-matter, duration, nature and purpose, the type of personal data and categories of data subjects and the obligations and rights of the controller. The same contractual obligations shall apply to any authorized processor's subcontractor, but if the latter fails to fulfill its data protection duties, the initial processor remains fully liable to the controller for the performance of that other processor's obligations. Such agreements set out to increase the transparency of the processing between the parties of the contract (cloud client, cloud provider, subcontractors) and, at the same time, between the data client and data subject, which may effectively know who is handling the data and where.

A responsibility to ensure an appropriate level of security is now addressed at Art. 32, GDPR: together with the controller, the data processor has to evaluate the risks inherent in the processing, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected, and implement measures to mitigate those risks. In particular, GDPR includes as appropriate measures: a) the pseudonymisation and encryption of personal data; b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. This list is not exhaustive and, in line with the abovementioned principle of technological neutrality, the GDPR prefers to suggest some elements for conducting a data security assessment, such as: accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage. CPs shall thus conform and update their security measures in the light of the technological development, following for example the best practices encouraged by influential expert groups, such as the European Union Agency for Network and Information Security.

The liability of the processor is now explicitly stated at Art. 82, GDPR, according to which any person who has suffered material or non-material damage as a result of an infringement of the GDPR is entitled to receive compensation from the controller or processor for the damage suffered. The processor shall be liable for the damage caused by processing only where it has not complied with obligations of the Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. It is a hypothesis of aggravated liability, since the person who caused the damage may be exempt if he or she proves of not being responsible in any way for the event giving rise to the damage. The right to compensation of the data subject is ensured by the rule of joint liability in case of more than one controller or processor, or both a controller and a processor, are involved in the same damaging conduct: they shall be held liable for the entire damage, without prejudice to the recourse action by the one who paid against the co-debtors according to their part of responsibility for the damage.

Other processor's obligations consist in assisting data controller in its tasks and responsibilities, such as, for example, the duties to: notify the controller in case of data breaches without undue delay after becoming aware of a personal data breach (Art. 33.2, GDPR); cooperate with the supervisor authority (Art. 31, GDPR); provide all information necessary to demonstrate the compliance of the controller with its obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (Art. 28.3.h, GDPR); ensure

compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority (whereas 95, GDPR).

The GDPR aims at solving also another critical issue for our topic, considering how complex the cloud supply chain may become: the Regulation now provides a clearer set of provisions for governing the application of EU data protection law outside the EEA boundaries. According to Art. 3, GDPR shall apply not only when data processors and controllers are established in the Union, but also in the case they are not established in the EU and their processing activities are related to: a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or b) the monitoring of their behavior as far as their behavior takes place within the Union. This means that data protection rules may apply also to extra-EU data processors, when their business is substantially directed to European citizens.

As said, business models in the context of cloud computing may be different and particularly articulated: in some cases, CPs act as proper data controllers (if, for example, proceed to the processing for their own purposes, such as statistical or research purposes), or, in other cases, as joint-controllers if they determine the purposes and the means of the processing, in combination with any other controller. In the latter case, the GDPR expressly states that joint-controllers must in a transparent manner determine their respective roles, responsibilities and relationships, by means of an arrangement between them. The design of the contract is then crucial to clearly allocate accountability.

Lastly, the GDPR strengthens the rules regarding the cross-border data transfer, which is now particularly topical after the ECJ decision in the Schrems case [14]: the Regulation confirms the necessity that data transfer outside non-EU Member States may take place not only to third countries, but also to a territory or a specified sector within a third country, or to an international organization, whose level of data protection has been considered "adequate" by the EU Commission; in the absence of the adequacy decision, cross-border data transfer may occur under appropriate safeguards, which include the adoption of binding corporate rules or standard contractual clauses elaborated by the Commission or a supervisory authority (Art. 46.2, GDPR). It is worth nothing that in the regime of derogation for specific situations (Art. 49, GDPR), cross-border data transfer may take place with the consent of the data subject, but - unlike Directive 95/45/EC - such a consent must be explicit and informed about the possible risks of the transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.

A. Specific obligations for the processing of health data

The GDPR is going to innovate the provisions concerning the processing of health data. Firstly, the Regulation introduces the notion of data concerning health, which are defined as personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status (Art. 4.15, GDPR). Such a concept has to be interpreted broadly, since it refers to all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes also administrative information collected in the course of the registration, the unique identification number of patients, information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples, and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject regardless of the source that produces it (whereas 95, GDPR).

Considering their sensitivity, the GDPR provides a series of additional obligations when the processing concerns health data:

1) to lawfully process such kind of information, it is necessary the explicit consent of the data subject or, alternatively, the conditions set forth in Art. 9.2, GDPR;

2) automated individual decision-making (Art. 22) shall not be based on health data, unless the data subject has given the explicit consent or the processing is necessary for reasons of substantial public interest and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place;

3) a data protection impact assessment must be carried out if the processing of health data is on a large scale;

4) where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data, they shall designate a data protection officer (Art. 37, GDPR);

5) data processors shall maintain written records of all categories of processing activities carried out on behalf of a controller, containing information listed in Art. 30.2, GDPR.

III. OPEN ISSUES

The long-awaited GDPR introduces several changes to the actual data protection laws, in the effort to update the regulatory framework to challenges of the information age. It lays down new protection measures for EU data subjects, increases the thresholds of accountability both for controllers and processors - establishing significant fines and penalties in case of violation of its rules - makes more clear the issue of applicable law and the requirements for transborder data flow. However, the Regulation has raised some criticisms [15-21] and some authors have provocatively wondered whether the new provisions might kill the emerging cloud industry [22]. Indeed, the GDPR leaves open serious questions and shortcomings, especially in the context of cloud for e-health solutions.

Firstly, the harmonization efforts represented by the enactment of a regulation are likely to be frustrated by the wide discretion left to the Member States. The latter shall in fact maintain or introduce national provisions to further specify the application of the GDPR, also for the processing related to genetic data, biometric data or data concerning health. So, the threat of uneven national provisions and, as a consequence, of

barriers to the information flow within the digital market potentially remains.

Secondly, the cornerstone of the new GDPR is still the blurred distinction among the actors of the processing (controller-processor) [15], while the realities of many cloud ecosystems is much more complex, dynamic, and involve multiple services and intermediaries [17-19]. To reiterate the rigid classification of the Directive, the binary model controller-processor (see, for instance, Art. 28.10, GDPR), and the "instructions" requirement does not seem to seize all the possibilities of current ubiquitous computing. Furthermore, we must note that despite the additional rights recognized to individuals by the GDPR, the role of the data subject appears to be inadequate in the light of the citizen-empowerment allowed by smart technologies, thanks to which the person is called upon to participate actively in her information privacy, by contributing in some cases to co-determine means, conditions or purposes of the processing. ICT and the potential of s-Health require policy makers and lawyers to re-think the pyramid of the data protection actors, since it does not reflect the digital architectures of the processing and the effective powers of the subjects involved.

The problem of the asymmetry of power between controllers and processors is exacerbated in the context of cloud: "certain clauses in the model do not reflect and may not fit into the technical and organizational frameworks of cloud services. For instance, the assumption that the data controller is the strong, controlling party that has the actual ability to instruct and control the processor (cloud providers, for example) may be illusory. Provisions requiring the processor to submit its facilities for audit by the controller and supervisory authorities are less feasible in the cloud, in view of the millions of customers a cloud provider may have. It is also less likely that a cloud service provider will first obtain prior written consent from all of its customers before engaging in every support service, where those are regarded as sub-processing" [17]. In addition, considering that CPs tend to offer a standard service, the need to conduct an impact assessment for adapting the level of security according to the controller's needs may lead the CPs to the behavior of implementing the highest level of protection for every processing. This may result in a considerable increase in costs, which pass on to the customer, even though her processing did not entail high risks.

IV. Conclusion

Over the next two years, CPs will have to revise their business, processes and contracts according to the big changes brought by the data protection reform. In order to ensure a better protection for the rights and the liberties of individuals in the information society, the GDPR has introduced additional provisions, which will affect also the processing via cloud. In the paper a short guidance of the new main obligations for CPs has been offered. However, despite the efforts of the new Regulation some critical issues, peculiar of the cloud environment, remain unresolved. The solution of these key points will be crucial for an effective protection of data subjects and a wide uptake of cloud for s-health.

References

[1] Communication from the Commission to the European Parliament, the Council, the EESC and the Committee of the Regions, "Unleashing the Potential of Cloud Computing in Europe," COM/2012/0529 final.

[2] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, "e-Health cloud: opportunities and challenges," Future Internet, vol. 4, no. 3, pp. 621–645, July 2012.

[3] A. Solanas et al., "Smart health: a context-aware health paradigm within smart cities," Communications Magazine, IEEE, vol. 52, no. 8, pp. 74–81, August 2014.

[4] A. Holzinger, C. Röcker, and M. Ziefle, "From smart health to smart hospitals," in Smart Health Open Problems and Future Challenges, A. Holzinger, C. Röcker, and M. Ziefle, Eds. Berlin: Springer, 2015, pp. 1–20.

[5] L. Hood and S.H. Friend, "Predictive, personalized, preventive, participatory (P4) cancer medicine," Nature Reviews Clinical Oncology, vol. 8, no. 3, pp. 184-187, March 2011.

[6] Y. Liang, N. Guo, C. Xing, Y. Zhang, and C. Guo, "Chronic Knowledge Retrieval and Smart Health Services Based on Big Data," in Smart Health International Conference, ICSH 2015 Phoenix, AZ, USA, November 17–18, 2015, X. Zheng, D. Dajun Zeng, Hs. Chen, S. J. Leischow, Eds., Springer, 2015, pp. 231–240.

[7] European Commission, "The Future of Cloud computing. Opportunities for European Cloud Computing Beyond 2010," 2010.

[8] Art. 29 Working Party, "Opinion 05/2012 on Cloud Computing," adopted July 1 st, 2012.

[9] Italian Data Protection Authority, "Cloud computing: indicazioni per l'utilizzo consapevole dei servizi," adopted June 23 rd, 2011.

[10] Italian Data Protection Authority, "Cloud computing - proteggere i dati per non cadere dalle nuvole," adopted May 24 th, 2012.

[11] D. Ding, M. Conti, and A. Solanas, "A Smart Health Application and its Related Privacy Issues," in Proceedings of the 2016 Smart City Security and Privacy Workshop (IEEE CPS Week workshop: SCSP-W 2016), to appear, Vienna, Austria, April 11, 2016.

[12] Art. 29 Working Party, "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing," adopted September 22 nd, 2015.

[13] P. Balboni and F. Fontana, "Cloud computing: a guide to evaluate and negotiate cloud service agreements in the light of the actual European framework," ICT Law Review, vol. 1, pp. 12-17, 2013.

[14] Judgment of the Court (Grand Chamber) of 6 October 2015, Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650.

[15] P. De Hert and V. Papakonstantinou, "The new General Data Protection Regulation: still a sound system for the protection of individuals?" Computer Law & Security Review, vol. 32, no. 2, pp. 179 -194, April 2016.

[16] W.K. Hon, C. Millard, and I. Walden, "The problem of 'personal data' in cloud computing - what information is regulated? The cloud of unknowing, part 1," International Data Privacy Law vol. 1, no. 4, pp. 211-228, March 2011.

[17] I. S. Nwankwo, "Missing links in the proposed EU data protection regulation and cloud computing scenarios: a brief overview," JIPITEC, vol. 5, pp. 32-38, 2014.

[18] P. Blume, "Controller and processor: is there a risk of confusion?," International Data Privacy Law, vol. 3, no. 3, pp. 140-145, February 2013.

[19] B. Van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC," Computer Law and Security Review, vol. 28, no. 1, pp. 25-43, February 2012.

[20] B.J. Koops (2014), "The trouble with European data protection law," International Data Privacy Law, vol. 4, no. 4, pp. 250-261, October 2014.

[21] G. Hornung, "A general data protection regulation for Europe?" SCRIPTed, vol. 9, no. 1, pp. 64-81, April 2012.

[22] W.K. Hon, "GDPR: Killing cloud quickly?," Privacy Perspective, Iapp.org, March 17 th, 2016.