diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 09/03/2017

All'indirizzo http://www.diritto.it/docs/39147-eba-rts-technical-standard-about-security-of-payments-under-psd2-the-gdpr-perspective

Autore: Marcoccio Gloria

EBA RTS Technical Standard about security of payments under PSD2 & the GDPR perspective

EBA RTS Technical Standard about security of payments under PSD2 & the GDPR perspective

by Gloria Marcoccio - gloria.marcoccio@glory.it

Introduction

The European Banking Authority (EBA) published on February 23 the final "*Draft regulatory technical standards (RTS) on strong customer authentication and common and secure communication under Directive 2016/2366 (PSD2)*"[1], as a result of its reviews and amendments on the first RTS draft version submitted to open consultation - ended In October 2016, where EBA received 224 responses from many stakeholders and payments market operators.

EBA has developed the RTS according to Article 98 of the EU Payment Services Directive 2015/2366 (PSD2)[2]. The RTS is one of the Delegated Act under PSD2 and it shall be officially issued as an EU Regulation, therefore directly in force and applicable in all the EU Member States without need of any transposition into each country legislation framework.

The EU Commission will carry out a legal review before adopting the RTS, with the EU Council and EU Parliament having scrutiny rights in such process: EBA expects the RTS Regulation will be applicable at the earliest in November 2018 i.e. 18 months after its entry into force, expected in May/June 2017.

The RTS aims to lay down the result of complex trade-offs between the various objectives of the PSD2, such as enhancing security, facilitating customer convenience, ensuring technology and business-model neutrality, contributing to the integration of the European payment markets, protecting consumers, facilitating innovation, and enhancing competition through new payment initiation and account information services.

The RTS requirements are expressed in terms of:

- Strong Customer Authentication (SCA) and related security measures to be implemented (Articles 2-9)
- Exemptions from SCA, in particular for: Payment Service user accessing limited only Payment account information, Contactless payments at point of sale, Transport and parking fares, Trusted beneficiaries and recurring, Payments to self, Low value transaction (Articles 10-18)
- Confidentiality and integrity of the payment service users' personalized security credentials (Articles 19-24)
- General requirements for communication (Articles 25-26) and
- Specific requirements for the common and secure open standards of communication (Articles 27-31)

As a whole the RTS requirements shall have meaningful implementation impacts in terms of technical, procedural and organizational measures under the liability of the Payments Service Providers (PSP) subject to the PSD2, therefore the 18 months of the intervening period provides the industry with time to develop the necessary standards and or technological solutions that are compliant with the EBA's RTS.

[1] http://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2. In the year 2014 EBA issued another important document about the security in Internet payments: EBA/GL/2014/12 accessible at: https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29_Rev1

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366

EBA RTS from the GDPR perspective

The RTS makes express reference to the EU Regulation 2014/910[3] (known as EIDAS Regulation) in relation to qualified certificate for electronic seals or website authentication involved in the provision of a Payment Service (PS), however this is without prejudice to the PSPs obligations of compliance with other applicable legislations, as in the case of personal data protection.

Indeed, the payment service operational processes and the ones involved in the implementation of the measures required to fulfill the RTS requirements require the processing of large amount of several type of personal data of the PS users (the Data Subjects according to the terminology of the European Data Protection Law).

For this reason it is interesting to underline some of the essential aspects of the RTS, read from the perspective of the new European data protection law, i.e. the EU Regulation 2016/679[4] (known as GDPR-General Data Protection Regulation), in force from 25 May 2016, it shall apply from 25 May 2018. The GDPR will repeal the 22 years old EU Privacy Directive 95/46/EC and, being a Regulation, it is directly applicable in all the EU Member States.

According to the definition of Personal Data[5], many of the data processed for the purpose of the RTS implementation (although not obvious as is the case of IP address of the PS user's device - personal computer, smartphone,..) and many of the elaborations required by the RTS involve particular processing of Personal Data, subject to specific GDPR provisions.

In fact the RTS requirements involve monitoring and profiling of the behaviour of the PS users in order to mitigate the risk of fraud and in general of illicit use of PSs, both in the case of the application of SCA and when the PSPs can make use of SCA Exemptions. Furthermore the RTS requires the implementations of security measures specifically identified (for example in the cases of Articles 4, 5, 30,...) as well as implementation of security measures commensurate to specific risks (for example in the cases of Articles 6, 7, 8, 20, 25,...).

Here below a summary overview of some of the main GDPR provisions applicable to the processing of personal data performed by PSPs for RTS purposes, please note that breaches of GDPR provisions are sanctioned up to 20 million eur or 4% of the annual turnover if greater.

Legal Ground and Data Subject Information and Rights

RTS, as Regulation, it will provide the essential Legal Ground in order the PSPs can lawfully perform the personal data processing required by the RTS itself (GDPR Article 6(1)(c), i.e. '*processing is necessary for compliance with a legal obligation to which the controller is subject*'. This means that the PSPs will not require the consent of the PS users for processing their personal data under RTS, nor they have to constraint the processing to a contract between PSP and PS user. The RTS processing involves *'Automated individual decision-making, including profiling'* especially when the PSPs are required to monitor some dynamic parameters and characteristics of a transaction and/or take decision on the past behaviour of a PS user for example: for having in place transaction monitoring mechanisms for detecting unauthorised or fraudolent payment transactions or for the purpose to apply the SCA exemption for '*Low value transaction*'.

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2016%3A119%3ATOC&uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG

[5] GDRP Article 4(1): "*'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*"

In this context, due to the legal ground based on the need to comply with a legal obligation, it is not applicable the Data Subject right '*not to be subject to a decision based solely on the automated processing including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'* (GDPR Article 22).

Such legal ground is valid insofar the PSPs process the data exclusively for the purpose to fulfill the RTS: any other different usage of the data collected and processed for RTS purpose will require the existence of an appropriate legal ground: please consider that consent and contract legal ground could expose the PSP to the application of particular GDPR requirements such as for example the need to fulfill the Data Portability, one new important and controversial right enshrined by the GDPR (Article 20) to the Data Subjects.

The processing of such data for other purpose (GDPR Article 6(4)) could be lawful when based on a '*legitimate interest*' pursued by the PSP in its role of Controller (GDPR Article 6(1)(f)),however in this case the PSP has to perform an analysis (and be able to document it according to the principle of Accountability GDPR Article 5(2)) in order to ensure that its interest is not overridden by the interests or fundamental rights and freedoms of the Data Subjects.

In any case the PSPs have to provide the PS users in their role of Data Subject, suitable Information with regard to the processing of their personal data for RTS purposes, pursuant to GDPR Articles 13 and 14 and provide information on and implement the proper procedures in order to allow the exercise of the applicable Data Subject' rights (GDPR Articles 12 and 15-22).

Privacy Principles, privacy by design and by default and Record of processing activities

The PSPs have to ensure that processing personal data for RTS purpose shall respect the general privacy principles set forth with Article 5(1) of GDPR, i.e. lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.

The adoption of *Privacy by Design and Privacy by Default* procedures pursuant to GDPR Article 25 is fully applicable to the processing performed for RTS purposes, and such processing shall be properly documented in the Record of processing activities pursuant to GDPR Article 30.

Security measures

All the RTS requirements are about security measures, in general well tuned with the GDPR Article 32 'Security of processing'. Nevertheless all the provisions contained in such Article have to be followed by the PSPs, for instance also those requirements not explicitly mentioned in the RTS such as "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;" applied to the tools and media provided by the PSPs to the PS users in order to allow their interaction with the PSs (for example the routine to access a bank account on line). Furthermore, all the adequate security measures required by the RTS, to be identified as a result of a specific risk analysis (as example, RTS Article 6-9), in any case shall offer the appropriate level of security against the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Data Protection Impact Assessment

GDPR Article 35 requires the execution of a Data Protection Impact Assessment (DPIA) where the type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons. The case of PSs, in particular the adoption of the measures required according to the RTS, based on extensive use of monitoring and profiling of the PS users behaviour, being a necessary input to decisions such as blocking an user transaction if likely to result in a fraud attempt, requires the execution of the preventive DPIA, since the case is clearly covered by the GDPR Article 35 (3) - at least condition (a):

'a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;'

However pursuant to Article 35 (10) since the legal ground for RTS involved processing is the legal obligation (the RTS itself), the DPIA provisions shall not apply if the relevant authorities (such as EBA at EU level) or better a specific statement - to be inserted in the final text of the RTS to be adopted by the EU Commission-, explicitly states that the law regulates the specific personal data processing operation or set of operations in question and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

Data Breach

Last, but really not least, the requirements about Data Breach[6], GDPR Articles 33 and 34, shall apply in the context of the RTS involved processing, thus requiring the PSPs, in their role of Controllers, to:

- notify the breach to the competent Data Protection Authority, without undue delay and, where feasible, not later than 72 hours after having become aware of it,
- if occurring specific circumstances of high risks, communicate the breach to the Data Subjects. This obligation does not apply if the Controllers have implemented safeguards fulfilling the requirements stated in GDPR Article 34(3): the RTS measures could considered as whole, able to fulfill the requirement for such exemption, nevertheless, in my understanding, a specific statement in this sense it should be issued by the EU Banking Authorities avoiding to allocate such liability to the assessment mad by the single PSP in case of Data Breach
- implement a repository for documenting *'any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this* [Data Breach GDPR] *Article*'.

[6] GDRP Article 4 (12): *'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;*