Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States

Elizabeth Kennedy *, *Christopher Millard*

School of Law, Queen Mary University of London, London, United Kingdom

Keywords:
Data security
Cyber security
Authentication
Two-factor
Multi-factor
Data protection
Data privacy

A B S T R A C T

Ensuring the security of personal data, particularly in terms of access controls, is becoming progressively more challenging. The most widely deployed authentication method, a user name plus a password, increasingly appears to be unfit-for-purpose. A more robust technique for maintaining the security of personal data is multi-factor authentication whereby two or more different types of credential are required. This approach is gaining traction, and in the European Union, some national data protection authorities are already recommending the use of multi-factor authentication as a means of complying with the obligation in the EU Data Protection Directive to take "appropriate technical and organisational measures to protect personal data". A proposal to replace that Directive with a General Data Protection Regulation is at an advanced stage in the EU legislative process with enhanced data security a central feature of the proposed reform.

This article examines how the proposed Regulation would be likely to change the standard for data security both in general terms and in specific ways that might have an impact on the use of multi-factor authentication. Other sources of EU guidance are also considered, together with the position under the national laws and regulatory practices of six EU Member States.

1. Introduction

This article considers certain legal requirements relating to data security in the EU, and specifically the use of multi-factor authentication as a method of meeting the security obligations established by European Directive 95/46 EC on the processing of personal data (the "*Directive*"). Following this Introduction, the article comprises two sections: a discussion of the requirements of data security under European data protection legislation and a study of selected national positions. This article is an abbreviated version of a more detailed report which contains an Annex setting out in greater detail the position in each of the six EU Members States that are covered by this survey.

For the purposes of this article, *multi-factor authentication*, which includes *two-factor authentication*, is defined as follows:

A method of authentication which requires the user to have a combination of at least two out of the following three types of credentials:

(1) something you know (e.g. username, password, or PIN number);

E-mail addresses: c.millard@qmul.ac.uk. Home page: http://www.law.qmul.ac.uk/staff/millard.html. e.kennedy@qmul.ac.uk http://www.law.qmul.ac.uk/staff/kennedy.html.

* *Corresponding author.* School of Law, Queen Mary University London, 67-69 Lincoln's Inn Fields, London WC2A 3JB, United Kingdom.
E-mail address: e.kennedy@qmul.ac.uk (E. Kennedy).

http://dx.doi.org/10.1016/j.clsr.2015.12.004
0267-3649/

(2) something you have (e.g. a token such as an ATM card reader or one-time verification code which does not require a token); and
(3) something you are (e.g. biometric information like a fingerprint).

The focus of this article is on the legislative data security requirements and how multi-factor authentication may facilitate compliance with these obligations. We do not evaluate or comment on the effectiveness of multi-factor authentication as a security measure more generally. This article will not consider industry guidance and use of multi-factor authentication in specific sectors,[1] or the obligations of the data controller and data processor when a breach of security has occurred. At the date of writing, no final text of the General Data Protection Regulation (the "*Regulation*") has been adopted. Therefore, this article will refer separately to the texts of the Draft General Data Protection Regulation (the "*DGDPR*") adopted by the EU Commission,[2] EU Parliament,[3] and the General Approach of the Council of the European Union.[4] The transfer of personal data to third countries and related obligations as to data security will not be considered in this article. However, the provisions in Chapter V of the DGDPR on such transfers will be relevant for entities wishing to transfer data outside of the EU.

In the six Member States considered in this article, most national Data Protection Authorities ("*DPAs*") have issued guidance on the data security obligations of the Directive. Overall, for non-sectoral data protection, multi-factor authentication is not required to comply with the data security obligations; however, some identify multi-factor authentication as a method which may be used to comply. The position is slightly different in issued sectoral guidance. In three of the Member States surveyed,[5] compliance with industry standards is advised for the purposes of data security, and in many of these countries, multi-factor authentication methods are mandated as part of the industry standards. This suggests that some DPAs are already predisposed to suggest multi-factor authentication as a means of complying with the data security obligations despite the comparatively open requirements of the Directive. Notably, where a form of multi-factor authentication is mentioned, it is generally "two-factor authentication" and not "multi-factor authentication" which is referred to. This suggests that currently none of the relevant DPAs consider the use of three credentials necessary for authentication to comply with the Directive, but this may change as security threats and technologies evolve.

The Directive and the DGDPR both contain specific provisions detailing data security obligations which require the implementation of appropriate technical and organisational measures. On the whole, however, the DGDPR arguably mandates higher security requirements for personal data than the Directive. This is consistent with one of the DGDPR's main aims, which is to "strengthen privacy rights".[6] The DGDPR seeks to achieve this through various provisions which increase the "responsibility" and "accountability" of those processing personal data,[7] including a right to erasure[8] of personal data (right to be forgotten and to erasure),[9] more prescriptive obligations regarding data security,[10] data breach notifications,[11] data protection by design and by default,[12] and data protection impact assessments.[13] Although the obligation to notify data breaches is not examined in this article, the indirect effect of this provision for data security standards may prove to be significant as the mandatory[14] notification of breaches of personal data may encourage the pre-emptive adoption of more robust security measures for processing personal data.[15] This notification procedure is likely to increase the risk of reputational damage ensuing from a security breach. Moreover, the very substantial penalties envisaged under the DGDPR are likely to incentivise compliance generally, and specifically are likely to result in Data Controllers and Data Processors taking their data

[1] For example, in the banking, sector see European Banking Authority, Final Guidance on the Security of Internet Payments, EBA/GL2014/12. https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+(Guidelines+on+the+security+of+internet+payments)_Rev1.

[2] 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) (25.01.2012) COM(2012) 11 final. Referenced below as "Commission". http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf.

[3] European Parliament legislative resolution of 12 March 2014 on the 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) T7-0212/2014. Referenced in footnotes as "Parliament". http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bTA%2bP7-TA-2014-0212%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN.

[4] The Council has reached a "general approach" which means there is a political agreement in the Council on the basis of which it can begin negotiations; see http://www.consilium.europa.eu/en/press/press-releases/2015/06/15-jha-data-protection/; The Council 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) (11.06.2015) DOC no.9565/15 Referenced in footnotes as "Council". http://data.consilium.europa.eu/doc/document/ST-9788-2015-INIT/en/pdf.

[5] See France, the Netherlands, and Poland, below.

[6] Commission Fact Sheet, Data protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market (28.01.2015), MEMO 15–3802, http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm.

[7] See for example, Commission, Any Questions?: "how does the data protection reform strength citizens' rights?" (25.01.2012), http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf.

[8] Parliament, Article 17.

[9] Commission, Article 17.

[10] All three texts, Article 30.

[11] All three texts Article 31.

[12] All three texts, Article 23.

[13] All three texts, Article 33.

[14] The wording in the Council's text is more permissive than that of the Commission and Parliament.

[15] Information Commissioner's Office, "Implications of the European Commission's proposal for a general data protection regulation for business" final report (May 2013), at p. 40, https://ico.org.uk/media/about-the-ico/documents/1042341/implications-european-commissions-proposal-general-data-protection-regulation-for-business.pdf.