COMPUTER LAW & SECURITY REVIEW 34 (2018) 784–805

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

The GDPR: A game changer for electronic identification schemes? The case study of Gov.UK Verify

Sophie Stalla-Bourdillon[a,*], *Henry Pearce*[a,b], *Niko Tsakalakis*[c]

[a] *Institute for Law and the Web (ILAWS), University of Southampton, UK*
[b] *University of Hertfordshire, UK*
[c] *Institute for Law and the Web (ILAWS), & Web Science Centre for Doctoral Training, University of Southampton, UK*

ARTICLE INFO

Article history:

Keywords:
Data protection
Electronic identification
GDPR
Gov.UK Verify
Joint controllership
Legal bases

ABSTRACT

This article offers an interdisciplinary analysis of the General Data Protection Regulation (GDPR) in the context of electronic identification schemes. Gov.UK Verify, the UK Government's electronic identification scheme, and its compatibility with some important aspects of EU data protection law are reviewed. An in-depth examination of Gov.UK Verify's architecture and the most significant constituent elements of both the Data Protection Directive and the imminent GDPR – notably the legitimising grounds for the processing of personal data and the doctrine of joint controllership – highlight several flaws inherent in the Gov.UK Verify's development and mode of operation. This article advances the argument that Gov.UK Verify is incompatible with some major substantive provisions of the EU Data Protection Framework. It also provides some general insight as to how to interpret the requirement of a legitimate legal basis and the doctrine of joint controllership. It ultimately suggests that the choice of the appropriate legal basis should depend upon a holistic approach to the relationship between the actors involved in the processing activities.

1. Introduction

The General Data Protection Regulation (GDPR)[1] adopted by the European Union (EU) on 24 May 2016 will become applicable from 25 May 2018. It is intended to be a game changer for businesses operating within, or simply targeting, the EU Digital Single Market. Pursuant of this, we are now seeing the emergence of start-ups all over Europe promising to help businesses adapt to the evolving legal framework. Bigger companies have also been particularly eager to invest in staff training and compliance assurance mechanisms and processes. The strengthening of the arsenal of punitive sanctions for breach of its terms largely explains why the GDPR has been under the spotlight since its adoption.

Whether the GDPR should be seen as a regulatory revolution, has been heavily debated by legal practitioners and scholars since the beginning of its legislative process in 2012. It is certainly true to say, for instance, that the roots of many of the GDPR's substantive provisions can be traced to prior

* Corresponding author: The Institute for Law and the Web, Faculty of Business, Law and Art, University of Southampton, University Road, Southampton SO17 1BJ, United Kingdom.
E-mail address: S.Stalla-Bourdillon@soton.ac.uk (S. Stalla-Bourdillon).

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) [2016] OJ L 119/1.

https://doi.org/10.1016/j.clsr.2018.05.012

legislative instruments, notably the Data Protection Directive (DPD), which was adopted in 1995.[2] That said, the GDPR coming into force would mean that those already complying with the terms of the DPD would still necessarily have to modify some of their practices in order to continue to be compliant with some of the substantive tenets of the EU data protection framework. This is particularly true in respect of mechanisms and procedures relating to data subject rights, as the list of rights contained in the GDPR is more expansive than its DPD equivalent. However, what about the GDPR's other provisions? Have the rules relating to security measures that must be implemented by data controllers evolved as well? What about the restrictions concerning the choice of appropriate legal bases?

Just like the outgoing DPD, the GDPR applies to public authorities. As hinted above, most of the scholarly attention has focused on the implications of private actors having to comply with GDPR standards. Much less, however, has been written about the regulatory burden the GDPR imposes upon public authorities. Just like private sector organisations, public authorities can also be faced with data protection compliance issues. To pick just one example on 12 June 2017, the Information Commissioner's Office (ICO), the United Kingdom (UK) Data Protection Agency, fined Gloucester City Council £100,000 after a cyber attacker was able to gain access to council employees' sensitive personal information. Another legal saga has, arguably been more significant, despite not leading to any monetary penalty.[3] On 3 July 2017, the ICO ruled the Royal Free NHS Foundation Trust had not complied with the UK Data Protection Act when it provided patient data to Google DeepMind for the purpose of the clinical safety testing of the Streams application; it held the legal basis referred to by the Royal Free NHS Foundation to justify the repurposing of sensitive personal data was not appropriate.[4]

An observable trend in eGovernment initiatives throughout Europe in recent years has been the emergence and roll-out of electronic identity (eID) schemes that allow individuals to manage and authenticate their identities in conjunction with the use of online public services. Against this background, the UK Government has recently been developing its own eID scheme, Gov.UK Verify. This service, which delegates the verification of users' identities to a range of certified private companies, claims to provide a safer, simpler, and faster way of accessing government services.

The development of Gov.UK Verify can also be situated in the context of the encouragement of the deployment of eID schemes at the European Union level with the adoption two years before the GDPR of the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS)[5]. To be clear, eIDAS does not impose the creation of national eID schemes as such but aims to ensure their interoperability through the application of the principle of mutual recognition once Member States decide to notify them to the European Commission. Notably, eIDAS does not provide for recognition of eID schemes that belong to 'third-countries' (countries outside of the EU).[6] The UK invoked the exit process of Article 50 of the Treaty of the European Union on 28 March 2017, after the result of a referendum on 24 June 2016. 'Brexit', *i.e.* the UK leaving the European Union, is currently at the negotiating phase, with an expected 'exit day' on 29 March 2019.[7] Consequently, application of eIDAS after a potential withdrawal of the UK from the EU will largely depend on the outcome of the ongoing negotiations.[8]

eIDAS makes it clear that processing of personal data shall be undertaken in compliance with EU data protection law.[9] Obviously, data protection law meant in 2014 the DPD but eIDAS in some ways could be seen as anticipating the GDPR as one finds express references to key data protection concepts such as privacy by design.[10] Compliance with data protection law is a crucial requirement as the use of eID schemes as a means of managing identities necessarily involves the processing of individuals' personal data and, consequently, means that all such services must comply with EU data protection law. Importantly, Brexit should not affect this requirement. The message from the UK government and the ICO has always been that the substance of the GDPR will be part of UK law.[11] The strongest commitment to this ideal to date being the announcement of a new Data Protection Bill designed to transpose the terms of the GDPR into UK law.[12]

[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 [1995] OJ L 281/31.

[3] ICO Blog, News, <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/06/gloucester-city-council-fined-by-ico-for-leaving-personal-information-vulnerable-to-attack/> accessed 28 April 2018.

[4] Letter from Elisabeth Denam, Information Commissioner, to Sir David Solma (3 July 2017) <https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf> accessed 26 April 2018. The Streams application aims to detect signs of kidney failure at an early stage.

[5] Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73.

[6] In contrast, mutual recognition of trust services from third countries is possible under eIDAS Art. 14. In any case, despite the use of the terminology 'mutual recognition' it must be clear that notification of eID schemes is a one-way process: if a Member States puts forward a system, and takes liability, the others Member States have to accept it.

[7] European Union (Withdrawal) Bill 2017-19 HL Bill 79 at 40.

[8] See also fn. 77 and related discussion.

[9] eIDAS, Art. 5(1).

[10] Generally speaking, the term 'Privacy by Design' refers to an approach to the construction of technological communications systems, data processing technologies, and computer networks in which privacy is taken into account at all stages of the design process. On this topic, see Ann Cavoukian, 'Privacy by Design' (*Information & Privacy Commissioner of Ontario*, 2009) <https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf> accessed 26 April 2018.

[11] 'GDPR will come into force in the UK in 2018, minister confirms' (*Out-Law.com*, 9 November 2016) <https://www.out-law.com/en/articles/2016/november/gdpr-will-come-into-force-in-the-uk-in-2018-minister-confirms/> accessed 26 April 2018.

[12] Department for Digital, Culture, Media & Sport and The Rt Hon Matt Hancock MP, 'Government to strengthen UK data protection law' (*Gov.UK*, 7 August 2017) <https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law> ac-