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-

This article focuses on the issue of data protection law compliance in the context of eID schemes and examines Gov.UK Verify's compliance with some substantive provisions of the EU data protection framework. It identifies some inadequacies inherent in Gov.UK Verify's general setup in the light of the GDPR and ultimately argues that its operation lacks an adequate legal basis. In addition, despite the detailed allocation of roles between the different actors, this article suggests that the process of electronic identification by identity providers should lead to a situation of joint controllership.

Gov.UK Verify is therefore used as a case study to illustrate one key compliance challenge brought about by the GDPR: the establishment of a proper legal basis for the processing of personal data, which is relevant for both private and public entities. The choosing of an appropriate legal basis among the list of legal bases offered by GDPR Article 6 appears to be a crucial exercise for legal compliance purposes. Notably, the GDPR provides that

> *infringements of [the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9] shall …be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.*[13]

Interestingly however, in the Deep Mind affair, as hinted above, the ICO did not find the need to issue any monetary penalty, although several violations of the UK Data Protection Act were found to have occurred, one of which was the fact that Deep Mind's personal data processing activities were based on an erroneous legal basis. But that was prior to May 2018.

The legal assessment of Gov.UK Verify is then pushed further to assess whether the UK eID scheme involving both public bodies and private entities would not be better described as a situation of joint controllership and infer the consequences of such a characterisation.

This article thus consists of four main sections. The first section comprehensively outlines Gov.UK Verify, drawing attention to its technical and operational dimensions including the substance of the data protection impact assessment (the Verify DPIA). The second section sketches and discusses the various legal bases for the processing of personal data, a key constituent element of the EU data protection framework. The third section suggests that the processing of personal data by identity providers should be seen as one part of a whole set of processing activities and thereby adds an element of complexity to the picture by analysing the implications of the characterisation of the relationship between the different actors involved in the processing activities for the requirement of a legal basis. It thus provides insight as to how the concepts of legal bases and joint controllership should be interpreted in practice, which should have relevance for other cases of data processing and data sharing.[14]

cessed 26 April 2018. The Data Protection Bill was introduced to the House of Lords on 13 September 2017.

[13] GDPR, Art. 83(5).

[14] Of note, the ICO decided to assess Deep Mind's practices on the basis that Deep Mind was only a processor and not a data controller. See 'Collection: Data Protection Bill 2017' (*Gov.UK*, 14 September 2017) <https://www.gov.uk/government/collections/data-protection-bill-2017> accessed 26 April 2018.

2. Gov.UK Verify: a case study

In order to perform a legal assessment of Gov.UK Verify it is necessary to recall the inception of the project, describe its architectures, identify its actors, map the data flows between the different components of the system as well as give an account of the perceptions of those involved in the design of the scheme as to the data protection implications of the establishment of such an eID scheme.

2.1. *The history*

In the UK, plans for digital government have been annual since 1996, with the UK Cabinet Office pushing for an Identity Assurance Programme from 2010 to adopt federated identity assurance across government services. One of the central points of the 2013 UK 'Government Digital Strategy,' was to transition all public services to a 'Digital by Default' operation, where electronic transactions would be the default means of transacting with the public.[15] Action 11 of the Government's transformation plan promised that the Government Digital Service (GDS) would *"develop a framework to enable federated identity assurance to be adopted across government services in due course."*[16] Identity assurance came as a response to the previous failed attempt to introduce an identity card for all citizens, which would include a central 'National Identity Register' and an electronic identification functionality.[17] The National Identity Register was met with concern, and the plan for identity cards and the central Register were scraped with the Identity Documents Act.[18] Subsequent plans for electronic identification focused on software tokens and de-centralised approaches.

GDS' 'Identity Assurance Programme', later named 'Gov.UK Verify', was developed to replace the 'Government Gateway' platform, used to access most public services.[19] In the UK Digital Strategy for 2017, Gov.UK Verify is promoted as *"a federated, market-based approach to identity assurance for central government that can be reused in the wider public and private sectors."* [20]

[15] Cabinet Office, 'Government Digital Strategy: December 2013' (*Gov.UK*, 10 December 2013) <https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy> accessed 26 April 2018 *"Digital by default means digital services which are so straightforward and convenient that all those who can use digital services will choose to do so, while those who can't are not excluded."*

[16] *ibid*. Action 11.

[17] Identity Cards Act 2006, c 15, s. 1.

[18] Identity Documents Act 2010, c 40, ss. 1-3.

[19] 'What is the Government Gateway?' (*Government Gateway Help Desk*) <http://www.gateway.gov.uk/Help/Help.aspx?content=help_more_info_gateway.htm&languageid=0> accessed 26 April 2018.

[20] Department for Digital, Culture, Media & Sport, 'UK Digital Strategy 2017' (1 March 2017) <https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy> accessed 26 April 2018, ch. 6.

It has been designed around a set of 'Identity and Privacy Principles,'[21] focused on *"individual control and consent."*[22] An advisory group, whose purpose is to safeguard users' privacy, set up the principles.[23] Notably, the principles were written long after system design.

2.2. Architecture and actors

The premise underlying Gov.UK Verify's design is that eIDs should not be under the sole control of a central Governmental agency. The nine 'Identity and Privacy Principles'[24] form the minimum standard of the system's operation. The principles aim at a technology-neutral approach; they form targets the system should achieve but do not address specific means of how to achieve them. Gov.UK Verify centres on user choice: the user should be able to decide the number of eIDs they own and who holds the information about them.[25] Hence, the creation of an 'Identity marketplace' was decided. Although the marketplace is based on a public platform, a GDS owned and controlled hub, electronic identification of users is offered by private companies who act as Identity Providers.

Identity Providers have to be certified *"against common governance requirements,"* under the Identity Assurance Principle no. 7.[26] Certification, as outlined in the Framework Agreement,[27] is three-fold: certification against industry standards for information security,[28] certification that they meet government standards for identity assurance,[29] and comply with data protection law (certified through a Privacy Impact Assessment).[30] In relation to certification for identity assurance, the Framework explicitly mentions tScheme as the certification body.[31] tScheme is the *"Trusted List Scheme Operator (TLSO) and creates, hosts and maintains the UK's Trust Service-status List (TSL) on behalf of the Department for Business, Energy and Industrial Strategy (BEIS)"*[32] of the Qualified Trust Service Providers required by eIDAS.[33] It certifies Identity Providers against six 'Approval Profiles'[34] comprising assessment criteria. However, it seems that certification is not dependent upon meeting all six profiles. Some of the certified Providers do not satisfy the criteria of all Approval Profiles.[35] Surprisingly, it is not clear whether tScheme can issue the final 'operating as it is supposed to be' until the Identity Provider is actually operating. It is also interesting to note that not all providers in Gov.UK Verify's list are certified (namely, the Post Office does not hold certification from tScheme)[36] and that communication from GDS considers *"working towards independent certification"* an acceptable criterion to become a provider.[37] Electronic identification is organised in different 'Levels of Assurance' (LOA), a risk-based *"degree of confidence the government service requires that a user is who they say they are."*[38] Notably, Gov.UK Verify LOA have been criticised for being entirely one-sided: only one party, the government service provider, is getting identity assurance. The system uses software credentials for identification, a combination of *"usernames, passwords and security codes."*[39] Communication within the Gov.UK Verify feder-

[21] Privacy and Consumer Advisory Group, Identity Assurance Principles (v3.1, 2014) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1__4_.pdf> accessed 26 April 2018.

[22] *ibid*. 3.

[23] 'Privacy and Consumer Advisory Group' (*Gov.UK*) <https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group> accessed 26 April 2018 *"PCAG aims to ensure: users are in control of their information[;] information isn't centralised[;] users have a choice of who provides services on their behalf."*

[24] (1) The User Control Principle; (2) the Transparency Principle; (3) the Multiplicity Principle; (4) the Data Minimisation Principle; (5) the Data Quality Principle; (6) the Service-User Access and Portability Principle; (7) the Governance/Certification Principle; (8) the Problem Resolution Principle; (9) the Exceptional Circumstances Principle. *See* Privacy and Consumer Advisory Group, *Identity Assurance Principles* (n. 21).

[25] *ibid*. the Multiplicity Principle: *"I can use and choose as many different identifiers or identity providers as I want to."*

[26] *ibid*. p. 10.

[27] Cabinet Office, Framework Agreement and Schedules (Draft v0,9, 20 December 2014) <http://data.gov.uk/data/contracts-finder-archive/contract/1690273/> accessed 26 April 2018, p. 18.

[28] The Framework mentions ISO 27001 and ISO 15489-1, but accepts other equivalent standards: *ibid*. s. 8.10(g) and sch. 5(a)(2)(b).

[29] *ibid*. s. 8.10(f)j and sch. 5(a)(2)(a)(i).

[30] *ibid*. sch. 5(a)(2)(d).

[31] *ibid*. 83, although the government retains the right to change the certification body in the future: *"any organisation that has been approved for the assessment of trust services to the satisfaction of the Authority and that has been notified by the Authority as a Certification Body from time to time."*

[32] Department for Business, Energy and Industrial Strategy, Electronic Signatures and Trust Services (Guide, August 2016) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/545098/beis-16-15-electronic-signatures-guidance.pdf> accessed 26 April 2018, 9.

[33] 'UK's Trusted List' (*tScheme*, 2017) <http://www.tscheme.org/UK_TSL/index.html> accessed 26 April 2018.

[34] Base Approval Profile (tSd0111); Profile for Identity Registration (tSd0108); Profile for Credential Validation (tSd0109); Profile for Attribute Registration (tSd0110); Profile for an Identity Provider (tSd0112); Profile for Credential Management (tSd0113): 'Digests of Approval Profiles for IdP-related Services' (*tScheme*, 2010) <http://www.tscheme.org/profiles/IdP_digest_2.html> accessed 26 April 2018.

[35] See for example Experian's Grant of Approval who satisfies four ('IDaaS service from Experian Limited: Grant of Approval' (*tScheme*, October 2016) <http://www.tscheme.org/directory/EXPN_IDaaS/index.html> accessed 26 April 2018) compared to Barclays' which satisfies five ('Barclays Identity service from Barclays Bank Plc: Grant of Approval' (*tScheme*, 30 June 2016) <http://www.tscheme.org/directory/Barclays/index.html> accessed 26 April 2018).

[36] GDS justifies this omission by explaining that the Post Office uses the system of another provider to offer its services and therefore the certification of the other provider is deemed enough: Comment from Janet Hughes to Mark (5 January 2016) <https://identityassurance.blog.gov.uk/2015/12/03/working-with-identity-providers-as-they-become-certified-companies/#comment-41610> accessed 26 April 2018.

[37] Alastair Williamson-Pound, 'Becoming a GOV.UK Verify certified company' (*Gov.UK Verify Blog*, 2016) <https://identityassurance.blog.gov.uk/2016/02/25/becoming-a-gov-uk-verify-certified-company/> accessed 26 April 2018.

[38] Government Digital Service, 'Gov.UK Verify Technical Guide' (*Gov.UK Verify Technical Guide documentation*, 2014) <http://alphagov.github.io/rp-onboarding-tech-docs/index.html> accessed 26 April 2018, Glossary of terms.

[39] *ibid*.

ation happens through the Security Assertion Markup Language (SAML 2.0)[40] and data are signed and verified through a Public Key Infrastructure (PKI).[41]

Gov.UK Verify's architecture thus comprises five key elements:

(1) The **Federation Hub**: A central infrastructure that mediates all interaction between users, Identity Providers and Services (or Service Providers). The Hub leases eID services from the private Identity Providers. The Hub acts as a broker between data exchanges. Identity Providers and Service Providers have direct communication only with the Hub, so that the Identity Provider remains unknown to the Service Provider and *vice versa*. The Hub ensures that the required LOA is adhered to and does not collect or store data beyond the current session (stateless operation).[42]
(2) The **Service Provider**: Service providers are the different public services that can request the electronic identification of the user in order to transact with them. At the moment, service providers in the Gov.UK Verify federation are solely governmental departments.[43]
(3) The **Identity Provider**: Identity providers are "[*p*]*rivate sector organisations, paid by the government, to verify that a user is who they say they are and assert verified data that identifies them to a government service.*"[44] They verify the user's identity against various authoritative sources, like the HM Passports Office and the Driving Licensing Authority.[45]
(4) The **Matching Service**: A middleware deployed at the Service Provider level whose purpose is to match the eID received by the Identity Provider to a local account in the Service Provider's database.
(5) The **Document Checking Service**: A supplementary service designed and operated by GDS, whose role is to check the official documents provided by the user against authoritative sources. Currently, checks are performed against the HM Passport Office or the Driver and Vehicle Licensing Agency.[46] The system returns an attestation of the authenticity of the documents to the Identity Provider, meaning that Identity Providers do not have to directly access official records. The Document Checking Service is not engaged in every eID transaction; instead, it is only needed for the registration of a new user with an Identity Provider. Besides, it has been criticised for not federating.

From this description, it thus appears that the Gov.UK Verify system involve four actors:

1. **GDS**, operating the Federation Hub and the Document Checking Service.
2. Government Services acting as relying parties, which request authentication (in the sense of verification of identity) and which host Matching Services also characterised as **Service Providers**.
3. Certified Companies acting as **Identity Providers**.
4. **Service Users**.

The typical user journey in Gov.UK Verify starts when a user requests an identification against a governmental service. The service sends an authentication request to the Hub (step 1, Fig. 1) indicating the requested LOA (at the moment Gov.UK Verify supports only LOA 2).[47] The request is signed by the Service Provider. The Hub prompts the user to select one of the available Identity Providers, depending on the available data the user has for verification. An authentication request is sent to the selected Identity Provider, signed by the Hub (step 2, Fig. 1). The Identity Provider verifies the user's identity according to the indicated LOA. The verified identity (the eID) is sent as a response to the Hub, signed by the Identity Provider (step 3, Fig. 1). The eID contains an 'authentication assertion' – encrypted for the Hub – which asserts that the user's identity is authenticated and contains contextual information including the LOA.[48] It also contains an 'Identity assertion', also encrypted for the Hub, containing two elements: the Matching Dataset and a Persistent Identifier. The Matching Dataset comprises the same standard fields for every eID.[49] The Persistent Identifier is a pseudo-random value generated by the Identity Provider and refers to the combination of the user and the chosen Identity Provider.[50] The Hub then sends the 'Identity assertion' to the Matching Service located at the Service Provider. The 'Identity assertion' retains the signature of the Identity Provider and is encrypted for the Matching Service (step 4, Fig. 1). The Matching Service then performs a series of attempts to match the 'Identity assertion' to a local user record, known as 'matching cycles'. The first cycle, 'cycle 0', starts when the Matching Service changes the Persistent Identifier to a hashed value, created from the combination of user, Identity Provider and Service

[40] Cabinet Office, Identity Assurance Hub Service SAML 2.0 Profile v1.2a (August 7 2015,) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/279643/Identity_Assurance_Hub_Service_Profile_v1.2a.pdf> accessed 26 April 2018. Nevertheless, discussion about moving away from SAML has taken place in the context of the Open Identity Exchange (OIX), a non-profit organisation comprising industry leaders from different sectors working on promoting the adoption and expansion of digital identity services.

[41] Identity Assurance Team, Identity Assurance Documentation (Release, November 13 2015,) <https://media.readthedocs.org/pdf/random/latest/random.pdf> accessed 26 April 2018, 50.

[42] *ibid*. Architecture.

[43] *ibid*. Glossary 'Relying party'.

[44] Government Digital Service, Gov.UK Verify Data Protection Impact Assessment (18th May 2016) <https://identityassurance.blog.gov.uk/wp-content/uploads/sites/36/2016/05/GOV-UK-Verify-DPIA-v1.0.pdf> accessed 26 April 2018, p. 10.

[45] David Black, 'Validating identity information against an authoritative source' (10 October 2014) <https://identityassurance.blog.gov.uk/2014/10/10/introducing-the-document-checking-service/> accessed 26 April 2018.

[46] GDS has announced its intention to expand on the sources used for the Document Checking Service, but further information has not yet been published: Janet Hughes, 'How we're working to increase the range of data sources available for GOV.UK Verify' (*Gov.UK Verify Blog*, 1 December 2014) <https://identityassurance.blog.gov.uk/2014/12/01/data-sources/> accessed 26 April 2018.

[47] Government Digital Service, 'Gov.UK Verify Technical Guide' (n. 38), 'Architecture.'

[48] *ibid*. 'How SAML works with Gov.UK Verify.'

[49] *ibid*. Glossary 'Matching dataset.'

[50] *ibid*. Glossary 'Persistent identifier (PID).'

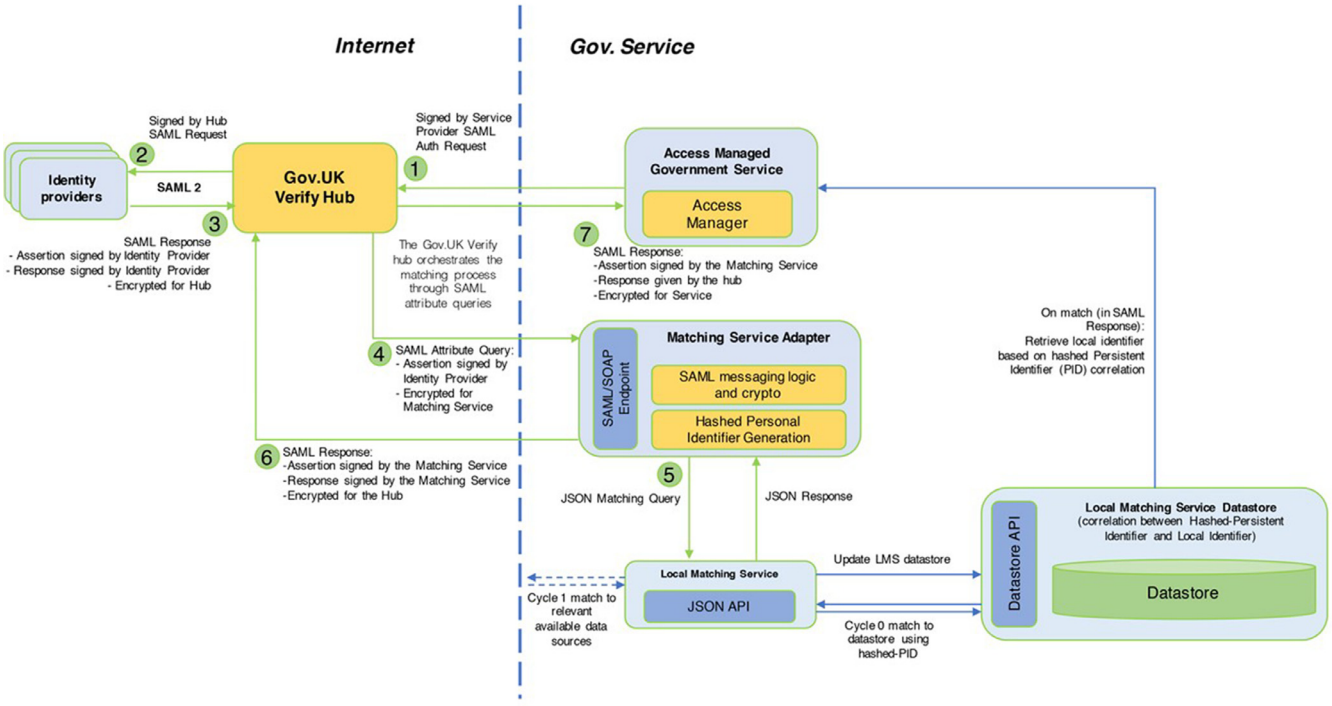

Fig. 1 – Gov.UK Verify actors and data flows.

Provider.[51] After creation of the hashed persistent identifier, the Matching Service checks whether the hashed value has already been associated to a user record in a local database. If a match is found, the 'Identity assertion' along with the hashed identifier are forwarded to the Service Provider. If not, the Matching Service tries to determine a match using the values of the Matching Dataset ('cycle 1'). Subsequent cycles, if no match is found, ask the user for additional attributes. When a match is found, the Matching Service sends a 'match' response along with the 'Identity assertion' back to the Hub, signed by the Matching Service and encrypted for the Hub (step 6, Fig. 1). The Hub sends the signed 'Identity assertion' in an encrypted form to the Service Provider (step 7, Fig. 1), which then retrieves the local record from its database.

2.3. *Gov.UK Verify data protection impact assessment*

While the Verify DPIA was obviously undertaken before 25 May 2018, the date at which the GDPR becomes applicable, it was published on 18 May 2016, after the public release of the final text of the GDPR, which was then adopted on 25 May 2016.[52] The authors of the Verify DPIA were thus fully aware of the content of the GDPR when they released the impact assessment. Besides, they changed the name of the document from privacy impact assessment to data protection impact assessment *"to reflect the terminology of the new EU General Data Protection Regulation."*[53] Despite this change and awareness, the drafters of the Verify DPIA recognised that a second impact assessment would have to follow to take into account the changes brought by the GDPR. It is therefore expressly mentioned that the Verify *"DPIA does not consider the requirements of the EU General Data Protection Regulation (GDPR), since the final text was only approved in May 2016."*[54] More than one year after, no new impact assessment has been released to the public.

The Verify DPIA is said to follow the approach advocated by the ICO in its code of practice on privacy impact assessment[55] but with the following caveat

> *it has been modified to take into account other specific requirements for the GOV.UK Verify environment, most notably the Identity Assurance Principles published by the Cabinet Office Privacy and Consumer Advisory Group (PCAG).*[56]

[51] *ibid*. Glossary 'Hashed persistent identifier (PID)': *"This ensures that identifiers for user identity are unique to specific services and can't be used across multiple services."*

[52] The first version of the data protection impact assessment is dated 27 January 2015. The document was then modified on 15 February 2015, 31 March 2016, and several times in May 2016 (13 May 2016, 16 May 2016 and 18 May 2016). An initial data protection impact assessment had been conducted in September 2014 for project approval purposes. Of note, the assessment for the beta system was released very late, when the system was finally declared live, although the private beta phase had started two years earlier.

[53] Government Digital Service, *Gov.UK Verify Data Protection Impact Assessment* (n. 44) 6.

[54] *Ibid* 7.

[55] ICO, Conducting Privacy Impact Assessments: Code of Practice (Version 1,0, February 2014). Note that the ICO guidance has evolved since then.

[56] Government Digital Service, *Gov.UK Verify Data Protection Impact Assessment* (n. 44) 6.

The approach is described as being aligned to the requirements of ISO27001 standards.[57] With this said, it is important to note that the Verify DPIA was produced fairly late in the process, during beta testing.

The Verify DPIA identifies three data controllers: GDS, the Certified Companies and Government Services.[58] While the pertinence of this assessment will be discussed below suffice it to note for now that under both the DPD and the GDPR a data controller is defined as: *"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"* with the caveat that *"where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."*[59]

As regards the legal basis, the justification for the processing as mandated by DPD Article 7 and by GDPR Article 6, two seem to emerge: consent and processing that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller:

> *GOV.UK Verify uses consent to enable processing, and processing is also enabled by Data Protection Act Schedule 2 Part 5 (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government, and (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.*[60]

Having said this, consent as a legal basis seems to be used for one type of processing and thereby one type of relationship: the processing undertaken by Certified Companies at the request of Service Users. One can read to that effect:

> *The Certified Company obtains consent to operate an account for the Service User, and to collect, share and maintain the personal information in order to verify and maintain the Service User's identity. The Certified Company obtains consent from the Service User to release matching data to the Federation Hub and on to the Government Service, at the request of the Service User.*[61]

The importance of consent in the relationship between Service Users and Certified Companies is also described as being the result of the implementation of the first identity assurance principle. The first identity assurance principle is formulated in these terms: *"I can exercise control over identity assurance activities affecting me and these can only take place if I consent or approve them."*[62]

Consent does not seem to be of possible use solely to Certified Companies however. To the question whether *"suppliers/partners have the right to use the personal information collected or shared under the service for their own purposes"*[63] it is answered that

> *Government Services may use information for their own purposes, but will have to disclose purposes and details of information required to the service user on a per-transaction basis, and seek appropriate consent.*[64]

Interestingly, the Verify DPIA does not use the terminology of eIDAS. eIDAS distinguishes between three types of actors for the operation of eID schemes: the notifying Member State, the party issuing the electronic identification means, and the party operating the authentication procedure. The electronic identification means is defined as per eIDAS Article 3(2) as *"a material and/or immaterial unit containing person identification data and which is used for authentication for an online service."* In the context of Gov.UK Verify Identity Providers are thus the parties issuing the electronic means even if a Matching Service sits within each (government) Service Provider. As regards the party operating the authentication procedure, the characterisation could seem less straightforward. Authentication *"means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed"* as per eIDAS Article 3(5). In the context of Gov.UK Verify, GDS should be the party operating the authentication procedure, to the exclusion of (Government) Service Providers.

From this introduction to the conception of the UK eID scheme, it thus appears that consent was and is still meant to play a prominent role in order to legitimise the processing of personal data for purposes of authentication. At the same time it is true to say that consent had never been thought as the sole legal basis contributing to the legitimisation of the processing. Still, as the GDPR does not exactly repeat the same words as the DPD it is worth verifying what the implications of the GDPR are or should be for the choice of an appropriate legal basis to then be able to assess the choices made by GDS.

3. Choosing the appropriate legal basis

The requirement of lawfulness of processing spans a relatively large range of legal bases. Only those that appear to be the most relevant for the activities of electronic identification within the framework of an eID scheme will be examined in this section:

- Consent;
- Processing that is necessary for the conclusion or performance of a contract to which the data subject is a party;
- Processing that is necessary for the performance of task carried out in the public interest or in the exercise of official authority vested in the controller;

[57] *ibid*. 7. Note that since the updated ISO/IEC 29100:2011 – Information technology – Security techniques – Privacy framework (International Organization for Standardization, Geneva, Switzerland, 2011) and ISO/IEC 29134:2017 Information technology – Security techniques – Guidelines for privacy impact assessment (International Organization for Standardization, Geneva, Switzerland, 2017) have been published, to conform with the new requirements of the GDPR.

[58] Government Digital Service, *Gov.UK Verify Data Protection Impact Assessment* (n. 10. See also Table 2: stakeholder analysis, 17.

[59] GDPR Art. 4(7). See also DPD Art. 2(d).

[60] Government Digital Service, *Gov.UK Verify Data Protection Impact Assessment* (n. 44) 10.

[61] *ibid*. 10.

[62] Privacy and Consumer Advisory Group, *Identity Assurance Principles* (n. 21) 8.

[63] *ibid*. 14.

[64] *ibid*.

- Processing that is necessary for the purposes of the legitimate interests of the data controller or other third party.[65]

The dual legal basis relied upon by Gov.Uk Verify is then assessed in the light of these development. This necessarily requires going back to the DPD in order to determine whether and how the GDPR goes beyond it.

Before focusing upon consent it is worth making clear why data protection compliance is crucial for the proper functioning of Gov.Uk Verify. EU data protection law imposes a range of substantive requirements on any act of data processing that involves personal data. Personal data is an expansive concept, which encompasses any information that can be related to an identified or identifiable individual and thus includes, but is not limited to, an individual's name, age, race, gender, sexual preferences, political affiliations, internet search histories, and health and financial information.[66] Processing is a similarly broad term, which is taken to encompass almost any form of personal data usage.[67]

Perhaps the most significant substantive requirement imposed by the EU data protection framework is the fact that the processing of personal data will only be considered lawful if one, or more, of a finite number of prescribed legitimising grounds for that processing can be identified.[68]

As mentioned in the introduction, it appears that Gov.UK Verify must comply with data protection law's substantive provisions. Firstly, as has been noted elsewhere, all data processing activities involving individuals' personal data that are undertaken by either private or public sector bodies fall within the scope of data protection law unless they have been specifically omitted, such as processing activities that are undertaken in conjunction with law enforcement proceedings.[69] At this point it is important to recall that Gov.UK Verify has a somewhat unusual structure in that it cannot accurately be described as a completely private or public sector service. Instead, Gov.UK Verify might best be described as a Public-Private Partnership, a term broadly used to refer to arrangements between government and private sector organisations in which partially or traditionally public activities are performed by the private sector.[70] Significantly, in this regard, however, as has been argued elsewhere, arrangements, which involve private parties entering systematic collaborative endeavours with governmental and other public sector bodies, will be subject to the same remit of data protection obligations as any other private or public party.[71]

Secondly, if it was not clear, eIDAS,[72] defines an interoperability framework of national eID management systems, which allows Member States to notify the European Commission of the interoperability of their national eID schemes, and demonstrate they conform to a number of substantive requirements, in order to make their schemes work cross-border.[73] Successful notification comes after a lengthy deliberation process.[74] Upon acceptance of the notified scheme, all other Member States are obliged to incorporate it into their individual authentication services.[75] Significantly, one notable requirement imposed by eIDAS is that in order to achieve successful notification any national eID scheme must comply with the substantive provisions of EU data protection law, with reference being made to the need to comply with the data minimisation principle.[76]

While, the UK government has never signalled its intention to notify Gov.UK Verify and has never explained how the requirement of including within the Minimum Dataset a unique permanent state-provided identifier could be met, it should tackle the challenge of data protection compliance in any case. The above considerations indicate that Gov.UK Verify must comply with the substantive provisions of EU data protection law, including the need for it to have a legitimate basis at all times for the processing of any personal data, irrespective of Brexit, although it remains to be seen what Brexit will bring for eID.[77] In this respect, whilst the data protection framework

[65] Other legal bases such *as "processing is necessary for compliance with a legal obligation to which the controller is subject"* and *"processing is necessary in order to protect the vital interests of the data subject or of another natural person"* as per DPD Art.7 (c) and (d) and GDPR Art. 6(c) and (d) are excluded from the scope of the analysis as they are not directly relevant for the context at hand.

[66] See DPD Art. 2(a) and GDPR Art. 4(1).

[67] See DPD Art. 2(b) and GDPR Art. 4(2); *Criminal proceedings against Bodil Lindqvist*, Case C-101/01, [2003] ECR I-12971 (EU:C:2003:596); *Bonnier Audi AB and others v Perfect Communication Sweden*, Case C–461/10, [2012] (EU:C:2012:219); *Michael Schwarz v Stadt Bochum*, Case C–291/12, [2013] WLR(D) 386 (EU:C:2013:670).

[68] DPD Art. 7 and GDPR Art. 6.

[69] Nadezhda Purtova, 'Between GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public-Private Partnerships' (2017) [pending] International Data Privacy Law ipx021 <https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipx021/4822279> accessed 16 August 2017; A. M. Klingenberg, 'Catches to the right to be forgotten, looking from an administrative law perspective to data processing by public authorities' (2016) 30 International Review of Law, Computers & Technology 67. See also Article 29 Data Protection Working Party, Opinion 06/2013 on open data and public sector information ('PSI') reuse (WP 207, 5 June 2013); Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119/89.

[70] Emanuel S Savas, *Privatization And Public-Private Partnerships* (Chatham House 2000), 4 (As adapted from Emanuel S Savas, *Privatization In the City: Successes, Failures, Lessons* (CQ Press 2005), p. 14).

[71] Purtova, 'Between GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public-Private Partnerships' (n. 69).

[72] eIDAS (n. 5).

[73] eIDAS Arts. 7 and 9.

[74] Niko Tsakalakis, Kieron O'Hara and Sophie Stalla-Bourdillon, 'Identity assurance in the UK: technical implementation and legal implications under the eIDAS regulation' (Proceedings of the 8th ACM Conference on Web Science (WebSci'16), Hannover, Germany, May 2016) <https://doi.org/10.1145/2908131.2908152> accessed 26 April 2018, 55-65.

[75] eIDAS Art. 6.

[76] eIDAS Rec. 11 and Art. 12.

[77] The European Commission has published a notice in preparation of UK's exit from the EU, outlining that "[a]s *of the withdrawal*

contains a number of grounds upon which the processing of personal data can be rendered legitimate, in the Gov.UK Verify context two legal bases have been put forward as explained in section 2: consent of the individual and performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.[78] At the same time consent has been the most publicised, which explains why the paper starts with this legal basis and carefully analyses both the DPD and the GDPR in order to highlight the changes brought by the latter.[79]

3.1. *Consent*

3.1.1. *The Data Protection Directive*

Article 2(h) of the DPD defines consent as "*…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.*"[80]

Article 7(a) then states that data may be processed when "*the data subject has unambiguously given his consent.*"

Accordingly, the giving of free, specific, informed and unambiguous consent is one way by which the processing of personal data can be rendered legitimate under the DPD.[81] In some ways the DPD's definition of consent could be considered somewhat restrictive, as it requires that the individual be clearly informed of what it is they are consenting to in advance of any consent being given. This approach is broadly in line with the existing data protection laws of most EU Member States, many of which have defined consent with similar restrictiveness.[82]

Conspicuously, the DPD's definition of consent is not phrased in terms of whether consent must be 'opt-in' (*i.e.* based on an affirmative act, such as clicking a box on an online form or providing a signature) or 'opt-out' (*e.g.* not unclicking a pre-ticked box). It has been debated whether the absence of the term 'explicit' indicates that opt-in consent is not required as a general matter.[83]

In this respect, it has thus been suggested that the DPD's definition is somewhat cryptic as well as restrictive, as the use of ambiguous terms like 'specific', 'freely given' and 'informed' allow for a broad spectrum of interpretation.[84] Moreover, the DPD says nothing in respect of the methods data controllers may, or should, use as a means of obtaining consent. However, Article 2(h)'s requirement that the data subject must "*signify*" their consent implies that complete inaction on behalf of the individual will not be sufficient to amount to valid consent.[85]

The Data Protection Act 1998 (DPA) transposed the terms of the DPD into the UK's domestic legal order. In accordance with what is said in the DPD, Schedule 2 of the DPA states that for the processing of personal data to be rendered lawful said processing must fall under one of the abovementioned legitimising grounds for processing, one of which is the consent of the individual. The DPA, however, contains no definition of consent, nor any guidance as to what is required to validly obtain it.

In lieu of any concrete guidance in respect of consent's interpretation being offered by the texts of the DPD and DPA themselves, the ICO, the UK's independent regulatory body responsible for matters regarding privacy and data protection, has offered its own views on how consent should be understood. Notably, in its 2017 guide to data protection, the ICO agrees that the DPD's inclusion of the word 'signify' means that an individual's consent must be actively communicated if it is to be considered valid, and that valid consent cannot be inferred from a failure to communicate. It is also expressly stated that any consent obtained by way of duress or misrepresentations will not adequately satisfy the conditions for the processing of personal data.[86] The ICO also advises that an individual's consent should be "*absolutely clear*", and that it must at the very least cover the types of information to be processed, the purposes of any processing, and any special aspects of that processing that may affect the individuals whose personal data are involved.[87]

date, electronic identification schemes which may have been notified by the United Kingdom before the withdrawal date pursuant to Article 9 of Regulation (EU) No 910/2014 will no longer be recognised by EU-27 Member States pursuant to Article 6 of Regulation (EU) No 910/2014.": European Commission, Notice to Stakeholders: Withdrawal of the United Kingdom and EU Rules in the Field of Electronic Identification and Trust Services for Electronic Transactions (Brussels, 21 March 2018) <https://ec.europa.eu/info/sites/info/files/notice_to_stakeholders_brexit_e_signature_final.pdf> accessed 14 April 2018, p. 2.

[78] Tsakalakis, O'Hara and Stalla-Bourdillon, 'Identity assurance in the UK: technical implementation and legal implications under the eIDAS regulation' (n. 74) 61.

[79] See e.g. Toby Stevens, 'GOV.UK Verify: privacy and consent' (*Gov.UK Verify Blog*, 30 July 2015) <https://identityassurance.blog.gov.uk/2015/07/30/gov-uk-verify-privacy-and-consent/> accessed 26 April 2018.

[80] DPD Art. 2(h).

[81] Explicit consent, a term which is not defined by the Directive, is required for the processing of data relating to the racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, or the health or sex life of the data subject: DPD Art. 8(2)(a).

[82] Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn, Oxford University Press 2007), 67.

[83] The Article 29 Working Party has suggested, however, that in certain situations an opt-in approach may be required. In an 'Opinion on unsolicited communications for marketing purposes' it stated that "*Implied consent to receive such mails is not compatible with the requirement of consent being the indication of someone's wishes, including where this would be done 'unless opposition is made' […] Similarly, pre-ticked boxes, e.g., on websites are not compatible with the definition of the Directive either*". See Article 29 Data Protection Working Party, Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC (WP 90, 27 February 2004), 5. Nevertheless, in certain jurisdictions, notably the United Kingdom, opt-out approaches to consent have previously on occasion been considered acceptable. See *Linguaphone Institute v Data Protection Registrar* [1995] (Case DA/94 31/49/1).

[84] Eleni Kosta, *Consent in European Data Protection Law* (Brill 2013), 109.

[85] Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (*n.* 82) 68.

[86] ICO, The Guide to Data Protection (v2,9,5, 7 July 2017) <https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-9.pdf> accessed 26 April 2018.

[87] *ibid.*

Additional guidance as to the interpretation of consent can also be found in UK case law. In *British Gas Trading v Data Protection Registrar*,[88] for instance, the British Data Protection Tribunal drew a distinction between new and existing customers of British Gas to determine when data protection law's consent requirement would be satisfied. The Tribunal held that new customers of the company would be taken to have consented to their personal data being used for the purposes of advertising if they had the option to opt-out in the initial contract for service. In respect of already existing customers, however, it was held that a failure to return an opt-out form would not amount to true consent.[89] Beyond providing enough information to the individual in order to allow them to express consent, in order for an individual's consent to be considered validly obtained the individual from whom the consent is sought must also be afforded a reasonable opportunity to express their consent, or the lack thereof.[90]

Outside of the field of data protection law, other UK cases have also provided some general guidance on the meaning of consent in other contexts, many of which correlate strongly with the abovementioned ICO guidance and data protection cases. As a general matter, it would appear, for instance, that in both criminal and civil law contexts for any consent to be considered valid the consenting individual must have been made fully aware of what it is to which they are giving their consent,[91] and that valid consent cannot be obtained by way of duress nor expressed through entirely passive acquiescence.[92]

The Article 29 Working Party has on occasion given its advice on consent's true meaning and how it should be understood in the data protection context. Notably, in its 2011 opinion on the definition of consent, the Article 29 Working Party examined the concept very closely, specifying several key criteria that must be met for an individual's consent to be considered valid.[93] The Article 29 Working Party concluded that only statements or actions that unambiguously indicated an individual's agreement would constitute valid consent. Whilst this did not specify whether consent must be 'opt in' or 'opt out', the clear implication was that the complete inaction of the individual would never be enough to amount to genuine consent.[94] Furthermore, it was made clear that for consent to be considered freely given, and therefore valid, notice must be provided to the individual in clear and understandable language prior to any processing of personal data occurring. Besides, in the event of an individual withdrawing their consent the data controller must delete any personal data pertaining to that individual unless another legal basis that justifies the storing of that data can be identified.[95]

3.1.2. *The General Data Protection Regulation*

The GDPR has been drafted as a means of bringing the EU data protection framework into alignment with contemporary data-handling practices and will be directly applicable and binding in full on all EU Member States from May 2018. As aforementioned, despite Brexit, the UK Government has confirmed it still intends to implement the substantive terms of the GDPR.[96] Significantly, for the purposes of this article, the GDPR retains the consent of the individual as a legitimising ground for the processing of personal data,[97] but contains a revised, and apparently narrower, definition of consent, which differs from its DPD equivalent. Specifically, the GDPR defines consent as

> *…any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*[98]

Upon first inspection, the GDPR makes no material change to the general principle that consent is one way in which the processing of personal data can be given a lawful basis and legitimised. However, if one is to analyse the GDPR's provisions relating to consent more thoroughly, particularly its recitals, it quickly becomes apparent that the GDPR makes it more difficult for data controllers to obtain valid consent than is the case currently under the DPD or DPA.

In Recital 32, for instance, it is specified that consent can be expressed by

> *…a written statement, including electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services, or another statement or conduct which clearly indicates the data subject's acceptance of the proposed processing of his or her personal data.*

It is also made clear in Recital 32 that "[s]*ilence, pre-ticked boxes, inactivity, a failure to opt-out, or passive acquiescence do not constitute valid consent*."

Recital 42 then states that

- [w]*here processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation.*
- *Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.*

[88] *British Gas Trading Ltd v Data Protection Registrar* [1998] 1 Info TLR 393, interpreting the 1984 Act.

[89] The judgment in this case seemingly echoed the Tribunal's earlier decision in *Linguaphone Institute v Data Protection Registrar* (n. 83).

[90] *Innovations (Mail Order) Ltd v Data Protection Registrar* [1992] (Case DA/92 31/49/1).

[91] See for example: *Re Caughey ex p. Ford* [1876] 1 ChD 521; *A-G's Reference (No 6 of 1980)* [1981] 2 All ER 1057; *R v Barnes* [2004] EWCA Crim 3246.

[92] See *Bell v Alfred Franks and Bartlett Co Ltd* [1980] 1 ALL ER 356.

[93] Article 29 Data Protection Working Party, Opinion 15/2011 on the definiton of consent (WP 187, 13 July 2011).

[94] This finding echoed an earlier judgment of the Court of Justice of the European Union (CJEU) in the *Bavarian Lager* case, where it was held that silence, or a failure to respond, could never form the basis of 'free and informed' consent. See *European Commission v The Bavarian Lager Co. Ltd.*, Case C-28/08 P, [2010] ECR I-06055 (EU:C:2010:378).

[95] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definiton of consent* (n. 93).

[96] *"GDPR will come into force in the UK in 2018, minister confirms"* (n. 11).

[97] See GDPR Rec. 40 and Art. 6(1).

[98] GDPR Art. 4(11).

- *…a declaration of consent preformulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.*
- *For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.*

Recital 43 further specifies that

In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority…

From this overview of the GDPR's provisions relating to consent, we can identify several notable ways in which obtaining valid consent is a more demanding task under the GDPR than it was the case under the DPD. This is something that has been acknowledged in the data protection literature, with various observers noting the GDPR's stricter consent requirements.[99]

The first obvious difference between the GDPR and the DPD is the fact that whilst under the DPD the data subject is required to signify their consent for it to be considered valid, under the GDPR the data subject will be required to express their consent by way of a statement or clear affirmative action. The obvious implication of this being that future consent must be obtained on an 'opt-in', rather than 'opt-out', basis if they are to be considered valid.

Secondly, whilst the DPD sheds very little light on the meaning of the phrase 'freely given', with most guidance in relation to this term coming in the form of Article 29 Working Party opinions, the GDPR makes it more challenging for data controllers to demonstrate that any consent obtained has been given freely. In particular, as noted above, under the GDPR data controllers are obliged to ensure that all data subjects have a genuine choice in respect of any prospective consent transactions to which they are subject. In addition, it is presumed that consent cannot be freely given, and therefore cannot form the legal basis for the processing of personal data, where there is a clear imbalance between the data subject and the data controller.

From the text of the GDPR itself, it is not immediately obvious what is meant by the term 'imbalance'. Some guidance as to its meaning can be found, however, in the recently published ICO guidance on the GDPR's consent requirements.[100] Particularly, the ICO advises that an imbalance of power will exist when an individual is reliant on another party for the provision of services, or fears adverse consequences linked to the withdrawal of those services, and feels they have no choice but to agree to whatever terms the service providers offers. Specifically, the ICO notes that relationships between employers and employees, as well as relationships between individuals and public authorities, are those in which a clear imbalance of power is likely to exist between the involved parties.[101] In other words, it would appear that an imbalance of power could be present where there is an observable inequality of bargaining power between two or more parties, due to the level of influence one has over the other.[102] It would therefore appear that the notion of 'imbalance' in the immediate context is comparable to its usage in other areas of EU law, notably those that deal with consumer protection.[103] In the fields of consumer and competition law, however, various observers have noted an apparent reluctance of the CJEU to articulate minimum standards of fairness and consumer protection, which, in turn, has impeded the development of a comprehensive understanding of the concept.[104]

In any event, as noted above, and as is alluded to by both the GDPR itself and the ICO guidance, imbalances of power are likely to be particularly prominent in situations in which the data controller is a public authority.[105] In fact, the GDPR appears to presume in Recital 43 that there is a clear imbalance between the data subject and the controller when the controller is a public authority. Significantly in this regard, however, though the GDPR makes numerous references to public authorities throughout its text, 'public authority', like 'imbalance', is a term that is not fully defined at any point. The underlying assumption should be nonetheless that interactions between public authorities and citizens are not optional: they are better described as being unilateral. This explains why they are not as a matter of principle regulated through contracts, even if consent as a data protection concept is distinct from the contract law concept of acceptance.

Some guidance as to the meaning of imbalance can, however, perhaps be inferred from CJEU case law outside the data protection field, although GDPR Recital 47 seems to suggest that Member States have a margin of appreciation. When addressing matters concerning the doctrine of direct effect in *A. Foster and others v. British Gas*,[106] for instance, the CJEU consid-

[99] See for example Bart W. Schermer, Bart Custers and Simone van der Hof, 'The crisis of consent: how stronger legal protection may lead to weaker consent in data protection' (2014) 16 Ethics and Information Technology 171, 171-182; Bart van der Sloot, 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) 4 International Data Privacy Law 307, 307-325.

[100] ICO, GDPR consent guidance (22 March 2018 - 1.0.65) <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent-1-0.pdf> accessed 26 April 2018.

[101] *ibid*. 14.

[102] To this end the ICO guidance can be said to correlate with earlier UK jurisprudence regarding the doctrine of inequality of bargaining power. See for example *Schroeder Music Publishing Co Ltd v Macaulay* [1974] 1 WLR 1308, 1316.

[103] Article 3 of Directive 93/13/EEC on unfair contract terms in consumer contracts specifies, for instance, that a contractual term which has not been negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer.

[104] See for example Michael Schillig, 'Inequality of Bargaining Power Versus Market for Lemons: Legal Paradigm Change and the Court of Justice's Jurisprudence on Directive 93/13 on Unfair Contract Terms' (2009) 33 European Law Review 336, 336-358. The ambiguity of the term has also been considered in the context of EU competition law. See Pinar Akman, *The Concept of Abuse in EU Competition Law: Law and Economic Approaches* (Hart Publishing 2012), 162.

[105] ICO, *GDPR consent guidance* (n. 100), 11; GDPR Rec. 43.

[106] *A. Foster and others v British Gas plc.*, Case C-188/89, [1990] ECR I-03313 (EU:C:1990:313).

ered the notion of 'emanation of the state', and remarked that it was a term that should be taken to refer to [at para. 22]:

> *…a body, whatever its legal form, which has been made responsible, pursuant to a measure adopted by the State, for providing a public service under the control of the State and has for that purpose special powers beyond those which result from the normal rules applicable in relations between individuals…*

Though the terms 'emanation of the state' and 'public authority' are not necessarily synonymous with one another, it seems highly probable that the former is broad enough to encompass the latter. More recently, in *Fish Legal*[107] the CJEU specifically considered the meaning of 'public authority' in the context of the Public Access to Environmental Information Directive,[108] which under Article 3 requires public authorities to provide environmental information upon request. Here, it was remarked that in order to determine whether a body constitutes a public authority it should be examined whether it possesses *"special powers beyond those which result from the normal rules applicable in relations between persons governed by private law"*.[109] The possession of such 'special powers', therefore, would likely indicate that a body was a public authority. The Court further observed that if a body is incapable of acting in a genuinely autonomous fashion, and that it cannot demonstrate that its provision of services is free from decisive influence of any governmental or public administrative organisations, this would also likely indicate that it was a public authority (at paras. 68 and 71). Notably, the UK Data Protection Bill includes a limited list of public authorities in its section 6 and refers to Section 3 of the Freedom of Information Act 2000 c. 36 for this purpose. It therefore builds upon, s. 1(1) of the UK Data Protection Act 1998, which states that the term 'public authority' in the data protection context should be defined in the same way as it is defined by Schedule 1 of the UK Freedom of Information Act 2000. The latter states that, amongst other institutions, government departments, The Competition and Markets Authority, The Office for Standards in Education, Children's Services and Skills, The Houses of Parliament, The Northern Irish and Welsh Assemblies, the armed forces, and local authorities should all be considered public authorities.

Thirdly, whilst the DPD fails to provide any details or guidance on the methods that can be used to obtain valid consent, the same cannot be said in respect of the GDPR. As noted above, the GDPR specifically recognises the validity of several methods that may be utilised by data controllers as a means of obtaining consent, ranging from verbal statements and written statements, to the ticking of boxes and the adjustment of technical settings. In so doing, the GDPR endorses the sentiment that different methods for obtaining consent may be more suitable than others in certain contexts, and compels data controllers to pick those that are most suitably aligned to their data processing practices. It is further made expressly clear that complete inaction or passive acquiescence on behalf of the data subject will never amount to genuine consent.

One final significant difference between the DPD and the GDPR relates to data controllers being able to demonstrate that they have obtained valid consent from data subjects. Whilst the DPD does not explicitly contain any requirement that data controllers must maintain evidence of any consents obtained from data subjects, the GDPR makes it clear that data controllers are formally required to be able to demonstrate that the consent they have obtained has been obtained validly. In situations in which a data subject and a data controller disagree as to whether consent has been validly given or obtained, therefore, the burden of proof will be on the data controller to demonstrate that this has occurred, which in turn will require an audit trail.

The abovementioned ICO guidance on the GDPR's consent requirements offers further clarification as to consent's interpretation.[110] Perhaps most interestingly, the ICO guidance specifically addresses the point that consent, as noted above, is only one of a number of legitimising grounds by which the processing of personal data can be rendered lawful, and that data controllers should only seek to rely on it in appropriate circumstances. In this respect, the guidance draws precise attention to the fact that, due to imbalances in power between parties, consent will, in the majority of circumstances, not be an appropriate legal basis for personal data processing operations undertaken by public authorities. It advises that public authorities should actively avoid relying on consent and seek to identify alternative legitimising grounds for the processing of personal data.[111]

In its recently released Guidelines on consent under Regulation 2016/679[112] intended to build on previous work, the Article 29 Working Party shed light upon the key elements of valid consent and in particular free/freely given. To quote Article 29 Working Party:

> *Recital 43 clearly indicates that it is unlikely that public authorities can rely on consent for processing as whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. WP29 considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities.*[113]

With this said, the Article 29 Working Party acknowledges that consent is not completely excluded for public authorities. In some circumstances, when data subjects are able to freely

[107] *Fish Legal and Emily Shirley v Information Commissioner and Others*, Case C–279/12, [2013] (EU:C:2013:853).
[108] Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC [2003] OJ L 41/26.
[109] *Fish Legal and Emily Shirley v Information Commissioner and Others* (n. 107) para. 52.
[110] ICO, *GDPR consent guidance* (n. 100).
[111] *ibid*. 2, 3, 19.
[112] Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679 (WP 259, adopted on 28 November 2017). These guidelines were last revised and adopted on 10 April 2018.
[113] *ibid*. 6.

refuse the processing, consent could be used, *e.g.* to share information about public roads via newsletters.[114]

3.2. *Processing that is necessary for the conclusion or performance of a contract to which the data subject is a party*

Both the DPD and GDPR specify that, other than relying on individual consent, the processing of personal data may lawfully take place when such processing is necessary for either entering or performing a contract with the individual to whom those data relate.[115] As has been noted elsewhere,[116] 'necessary' is an adjective that appears frequently in instruments such as the ECHR. Significantly in this regard, the jurisprudence of the European Court of Human Rights – which has been approved by the CJEU – has historically adopted an interpretation requiring that the practice in question be close to essential for the specified purpose.[117] The work of the Article 29 Working Party appears to suggest that a similar standard would be required in the data protection context if personal data were to be processed on this basis.[118] In other words, in order to legitimately process personal data on this basis, it would appear that data controllers must be able to show that it would be essentially impossible to enter into a contract, or perform a contractual duty in relation to a particular individual, without processing any of said individual's personal data. The requirement that the processing be 'essential' should also probably be read together with the principle of data minimisation.

This legitimising ground may be particularly relevant in situations involving a contractual agreement between an individual and a private party, such as a bank or insurance company. In such a situation, in order for the bank or insurer to be able to evaluate an individual's application for a loan or an insurance policy, the consideration of information such as the individual's name, date of birth and address will be integral to making such a determination.[119] Another salient example provided by the Article 29 Working Party is that the processing of personal data may be necessary for the performance of a contract of employment.[120] As others have noted, however, whilst it may be useful for an employer to record details of employees' next of kin in the event of accident or illness at work, this would not ordinarily be essential for the normal purposes of employment, and thus the identification of an alternative ground for processing would likely be required in such a context.[121]

3.3. *Processing that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*

The EU data protection framework also specifies that the processing of personal data is permissible when such processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest. Particularly, DPD Article 7(e) and GDPR Article 6(1)(e) both specify that processing will be lawful when it is "*…necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller…*"

Whilst neither the DPD nor the GDPR explicitly define the term 'public interest', both legislative instruments allude to the fact that matters concerning public health, social protection, taxation and customs administrations, humanitarian issues would fall within its scope.[122] This is an understanding of the term that is also alluded to by the Article 29 Working Party.[123]

The UK ICO has examined the notion of 'public interest' in the data protection context, and in its guidance on the public interest test in the context of the UK Freedom of Information Act 2000[124] states that:

> *The public interest can cover a wide range of values and principles relating to the public good, or what is in the best interests of society. Thus, for example, there is a public interest in transparency and accountability, to promote public understanding and to safeguard democratic processes. There is a public interest in good decision-making by public bodies, in upholding standards of integrity, in ensuring justice and fair treatment for all, in securing the best use of public resources and in ensuring fair commercial competition in a mixed economy…*[125]

Nevertheless, in its Guide to the General Data Protection Regulation, the ICO adds that

> *there is no direct link to the concept of 'public task' in the Reuse of Public Sector Information Regulations 2015 (RPSI). There is some overlap, as a public sector body's core role and functions for RPSI purposes may be a useful starting point in demonstrating official authority for these purposes. However, you shouldn't assume that it is an identical test.*[126]

The UK Data Protection Bill is more concise and includes in its section 7 processing of personal data that is *necessary for the administration of justice, the exercise of a function of either House of Parliament, the exercise of a function conferred on a person by an*

---

[114] *ibid*. 6.
[115] See DPD Art. 7(b); GDPR Art. 6(1)(b).
[116] See for example Ian Lloyd, *Information Technology Law* (Oxford University Press 2017), 108.
[117] See for example *Barthold v Germany* [1985] *7 EHRR 383*.
[118] See for example Article 29 Data Protection Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114, 25 November 2005), 12-14.
[119] Lloyd, *Information Technology Law* (*n*. 116) 108.
[120] Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context (WP 48, 13 September 2001), 8.
[121] Lloyd, *Information Technology Law* (*n*. 116), 109.
[122] See DPD Recs. 34 and 58; GDPR Rec. 46 and Art. 36(5).
[123] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248, adopted on 4 April 2017), 18.
[124] Freedom of Information Act 2000.
[125] ICO, The public interest test: Freedom of Information Act (v 2,1, 2017) <https://ico.org.uk/media/for-organisations/documents/1183/the_public_interest_test.pdf> accessed 26 April 2018.
[126] ICO, Guide to the General Data Protection Regulation (v 1,0,43, 22 March 2018) <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> accessed 26 April 2018.

enactment, or the exercise of a function of the Crown, a Minister of the Crown or a government department.

More broadly, away from the data protection field, notably in the context of issues relating to the free movement of goods, services, persons or capital, the CJEU has considered the term to encompass: the protection of public health; the protection of consumers, the protection of the environment; ensuring the integrity of the financial sector; the prevention of crime; the maintenance of financial and competitive balance; and the need to ensure the proper functioning of sporting competitions.[127]

GDPR Recital 41 clarifies that the public interest task legal basis does not necessarily require a legislative act adopted by a parliament. However, the law must be clear and foreseeable. To use the words of the ICO, *"the point is that your overall purpose must be to perform a public interest task or exercise official authority, and that overall task or authority has a sufficiently clear basis in law."*[128]

In its Guide to the General Data Protection Regulation, the ICO makes it clear that *"one key difference is that the GDPR says that the relevant task or function must have a clear basis in law."*[129] This is the consequence of GDPR Article 6(3).[130]

In addition, the task carried in the public interest legal basis is exclusive of the legitimate interests legal basis as per GDPR Article 6(1).

Irrespective of the definition of public interest itself, it is important to note that any processing of personal data undertaken on this basis may be subject to objections from individuals whose personal data are involved.[131] Once again, it is also important to pay heed to the DPD and GDPR's inclusion of the term 'necessary'. A clear apparent implication of this being that the processing of personal data in pursuit of performing a task that is in the public interest will not be permissible unless the achievement of said task be reached without the processing of personal data, or said processing cannot be legitimised by other means, such as the individuals whose personal data are involved giving their consent.

3.4. *Processing that is necessary for the purposes of the legitimate interests of the data controller or other third party*

The final legitimising ground for the processing of personal data listed by both the DPD and the GDPR is possibly the most extensive, and perhaps the most controversial. It sanctions the processing of personal data where it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.[132]

Whilst the DPD says little in respect of the meaning of 'legitimate interests', the recitals of the GDPR offer some insight as to its interpretation. Recital 47, for instance, specifies that a legitimate interest could exist where there is a *"relevant and appropriate"* relationship between the data subject and data controller, such as situations in which the data subject is a client of, or in the service of, the controller. As specific examples, the Recital also states that the processing of personal data for preventing fraud *"constitutes a legitimate interest"* and the processing of personal data for direct marketing may be regarded as being carried out for a legitimate interest. Recital 49 adds that the *"processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security"* also *"constitutes a legitimate interest."* However, in Recital 47 it is also made clear and emphasised that the legitimate interests of data controllers could be overridden by the fundamental rights of individual data subjects in situations where said individuals do not reasonably expect their personal data to be processed.[133] In other words, any processing of personal data that is undertaken based on the legitimate interests of the data controller will not be considered valid if said legitimate interests are outweighed by a need to protect the fundamental rights of individual data subjects whose personal data are involved. In this respect, it is important to note, therefore, that any existence of a legitimate interest will require a careful assessment in respect of any potential balancing that may be required in relation to any competing fundamental rights of affected individuals.

As aforementioned, Article 6(1) of the GDPR also makes it clear that this ground will not be applicable to processing carried out by public authorities in the performance of their tasks, though in this respect the abovementioned possible ambiguity as to the definition of the term 'public authority' must be kept in mind. Similarly, the abovementioned restrictions associated with the adjective 'necessary' must also be remembered.

Both the Article 29 Working Party and the CJEU have also considered the legitimate interest concept. In a 2014 opinion

---

[127] See for example *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein*, Case 120/78, [1979] ECR I-00649 (EU:C:1979:42); *Stichting Collectieve Antennevoorziening Gouda and others v Commissariaat voor de Media*, Case C-288/89, [1991] I-04007 (EU:C:1991:323); *Reinhard Gebhard v Consiglio dell'Ordine degli Avvocati e Procuratori di Milano*, Case C-55/94, [1995] I-04165 (EU:C:1995:411); *Union royale belge des sociétés de football association ASBL v Jean-Marc Bosman, Royal club liégeois SA v Jean-Marc Bosman and others and Union des associations européennes de football (UEFA) v Jean-Marc Bosman*, Case C-415/93, [1995] ECR I-04921 (EU:C:1995:463); *Vereinigte Familiapress Zeitungsverlags- und vertriebs GmbH v Heinrich Bauer Verlag*, Case C-368/95, [1997] ECR I-03689 (EU:C:1997:325); *Brian Francis Collins v Secretary of State for Work and Pensions*, Case C-138/02, [2004] ECR I-02703 (EU:C:2004:172); *Olympique Lyonnais SASP v Olivier Bernard and Newcastle UFC*, Case C-325/08, [2010] ECR I-02177 (EU:C:2010:143); *European Commission v Portuguese Republic*, Case C-543/08, [2010] ECR I-11241 (EU:C:2010:669).

[128] ICO, *Guide to the General Data Protection Regulation* (n. 126) 37—38.

[129] *ibid*. 36.

[130] See also GDPR Recital 45.

[131] See GDPR Recital 69 and Art. 6(1)(f).

[132] See DPD Art. 7(f) and GDPR Art. 6(1)(f).

[133] The possibility of individual data subjects objecting to their personal data being processed on the basis of the legitimate interests of a data controller is also explicitly mentioned by Recital 69 of the GDPR.

on the legitimate interests of data controllers, for instance, the Article 29 Working Party clarified both the words 'legitimate' and 'interest' in the data protection context. The Article 29 Working Party first suggests that 'interest' is not a term that is synonymous with 'purpose'. According to the Working Party, in data protection discourse the 'purpose' of a data processing activity is the reason or aim why any data are processed. Conversely, an 'interest' is the benefit that may be derived from that processing.[134] Secondly, the Article 29 Working Party suggests that the notion of a 'legitimate interest' is broad. Nevertheless, it lists some of the most common contexts in which the issue of legitimate interests may arise: the exercise of the right to freedom of expression; conventional direct marketing; unsolicited commercial messages; the enforcement of legal claims and debt collections; the prevention of fraud; employee monitoring; and the processing of personal data for historical, scientific or statistical purposes.[135] In summation of the above points, the Article 29 Working Party advises that in order to be relevant under data protection law, a legitimate interest must be: lawful (*i.e.* in accordance with applicable EU and national law); sufficiently clearly articulated to allow a balancing exercise to be carried out in relation to the interests and fundamental rights of affected individuals; and must represent a real and present interest, as opposed to one that is speculative.[136]

In the same opinion the Article 29 Working Party also advised that any balancing assessment a data controller is required to take in relation to their own legitimate interests and the fundamental rights of individuals should not in any way be thought of as straightforward or as a case of merely attempting to weigh and balance two easily calculable and comparable values. In addition, data controllers should not think of the legitimate interests condition as an 'open door' to legitimise their data processing activities.[137] Instead, the Article 29 Working Party suggests that making such a determination requires an extensive consideration of a number of factors, such as: the nature and source of the data controller's legitimate interest; the potential impact the proposed processing would have on the individual or individuals whose data were involved; and the existence or presence of any additional safeguards which could limit undue impact on these individuals (*e.g.* privacy enhancing technologies, increased transparency, rights to opt-out, and the right of data portability).[138] This advice on the potential complexity of making such assessments correlates strongly with what was said on the matter by the UK ICO in its 2014 discussion paper on big data and data protection.[139]

More recently, in *Rīgas satiksme*,[140] the CJEU also examined the legitimate interests ground for personal data processing. In particular, it considered the interpretation of the term 'necessary' and the question of whether the legitimate interests ground imposes obligations on data controllers to disclose the personal data of an individual to a third party for the purposes of allowing said third party to initiate legal proceedings against the individual. The conclusion arrived at by the CJEU was that the disclosure of an individual's personal data in such a scenario on the basis of the legitimate interests ground for processing would only be permissible, in cases where the fundamental rights of that individual do not take precedence. The CJEU also concluded that the legitimate interests ground for processing does not impose any obligations on data controllers to disclose personal data to third parties in situations such as that mentioned above, but merely permits them to make such disclosures in accordance with the national laws of the Member State in which they are based.

Of particular interest were the remarks of Advocate General (AG) Bobek, who suggested that the concept of a legitimate interest was *"elastic enough"* to encompass considerations other than a need to protect property, health, and family life, specifically, identifying the issuing of a legal claim as a particular example.[141] The AG seemingly re-emphasised the earlier guidance of the Article 29 Working Party by suggesting that as a part of any attempts to balance the legitimate interests of a data controller with the fundamental rights of an individual *"due consideration should in particular be given to the nature and sensitivity"* of the data involved.[142] In his concluding remarks, the AG also suggested that whilst the original and primary purpose of data protection law is the regulation of large-scale datasets involving personal data, *"a much lighter touch"* would be called for in situations involving datasets of a lesser size or individual pieces of information.[143] In so doing, the AG's comments appear to endorse a position of proactive reliance on the legitimate interests ground for personal data processing in appropriate circumstances. As has been remarked elsewhere, for instance, this position might be said to sit somewhat uneasily with the abovementioned Article 29 Working Party opinion, which urges data controllers not to think of the legitimate interests condition as an open door to legitimise their data processing operations.[144] Whether the CJEU entirely endorses its AG's approach is not clear either.

---

[134] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217, 9 April 2014), 24.
[135] *ibid*. 25.
[136] *ibid*.
[137] *ibid*. 49.
[138] *ibid*. 33.
[139] ICO, Big data, artificial intelligence, machine learning and data protection (v 2,2, 4 September 2017) <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed 26 April 2018.

[140] *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme", Case C-13/16, [2017] (EU:C:2017:336)*.
[141] *ibid*. at para. 65.
[142] *ibid*. at para. 69.
[143] *ibid*. at para. 98.
[144] Alison Knight, 'CJEU Advocate General Opines on the 'Legitimate Interest' Concept' (*Inforrm's Blog*, 5 February 2017) <https://inforrm.wordpress.com/2017/02/05/cjeu-advocate-general-opines-on-the-legitimate-interest-concept-alison-knight/> accessed 26 April 2018.

In its new guidance on legitimate interests, the ICO[145] clarifies that

> *Public authorities are more limited in their ability to rely on legitimate interests, and should consider the 'public task' basis instead for any processing they do to perform their tasks as a public authority.*
>
> *Legitimate interests may still be available for other legitimate processing outside of those tasks.*

It also adds that as a rule of thumb the legitimate interests basis is more appropriate in situations in which *"there's a limited privacy impact on the individual."*[146]

3.5. *Gov.UK Verify and its dual legal basis*

As aforementioned, the study of the content of the Verify DPIA concluded in 2016 shows that Gov.UK Verify is intended to be grounded upon two and not one legal bases,[147] although in public communications targeting Service Users consent has been presented as being the main legal basis. While the legal basis corresponding to the *"processing that is necessary for the task carried out in the public interest or in the exercise of official authority vested in the controller"* does not seem to raise many concerns, consent as the second (or probably first) legal basis creates some difficulties.

One key question is thus whether consent is a valid legal basis for the processing undertaken by Identity Providers. It is true that data subjects are offered a relatively limited choice of Identity Providers and that Service Providers also offer alternative means to access their services. However, there is a clear push towards 'digitalisation'.

In addition, one could argue that despite the fact that these Identity Providers are private companies there is a presumption of clear imbalance between the data subjects and the controllers in the same way as there seems to be a presumption of clear imbalance between data subjects and public authorities. There is indeed a very intimate relationship between Identity Providers and GDS. This raises the question whether Identity Providers could be assimilated to public authorities for the purposes of identification and authentication. First, Identity Providers are certified by tScheme.[148] Second, Identity Providers are actually paid by GDS.[149] Third, the relationship between Identity Providers and GDS is regulated through the means of a complex Framework Agreement, which includes a whole set of stipulations relating to reports, records and monitoring by GDS.[150] Interestingly, in most other Member States, the verification and confirmation of identity is undertaken by public authorities.[151] Although in many Member States the manufacturing of the infrastructure and the eID means (*e.g.* the cards) is outsourced to private entities (through tenders), the operation of identification and authentication is, in a majority of EU countries, under the responsibility of a governmental department.[152]

If we are to assume that there is such a thing as a (functional) EU concept of public authorities (which should be independent from national definitions), there is an argument that companies certified by GDS should also be considered public authorities themselves or at the very least performing a task carried out in the public interest. As noted above, for instance, the case law of the CJEU suggests that any bodies or institutions, irrespective of their legal form, that are responsible for providing a public service on behalf of the state, are afforded special powers or competencies by way of their relationship with the state, or are unable to act autonomously and in a way that is free from decisive influence of the state, must be considered public authorities. Companies certified by GDS could arguably be described as possessing some, if not all, of these characteristics. In any event, it is not necessary to identify a public authority for characterising an imbalance between the data subjects and the controllers.

Consent as a legal basis becomes even more problematic when used directly by (government) Service Providers. To the question whether *"suppliers/partners have the right to use the personal information collected or shared under the service for their own purposes"*[153] it is answered in the Verify DPIA that *"Government Services may use information for their own purposes, but will have to disclose purposes and details of information required to the service user on a per-transaction basis, and seek appropriate consent."*[154] Arguably, consent would only work if the processing activity was not necessary for the performance of a public task and data subjects were given realistic alternatives. For identification and authentication of Service Users in order to access government services, it would thus seem impossible to rely upon consent, as there is a strong argument that identification and authentication is necessary for the performance of a task carried out in the public interest, *e.g.* in order to prevent fraud. With this said, it would be better to interpret the task carried in the public interest ground narrowly and revert to the legitimate interests ground in this scenario to make sure a proper balancing is effectuated. Pushing the analysis further, it could

[145] ICO, Lawful basis for processing – Legitimate interests (v 1,0,0, 22 March 2018) <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/> accessed 26 April 2018.

[146] *ibid*. 22.

[147] Government Digital Service, *Gov.UK Verify Data Protection Impact Assessment* (n. 44), 10 and 25.

[148] Cabinet Office, *Framework Agreement and Schedules* (n. 27), sch. 5(a)(2) and sub-clause 8.10(f)(ii).

[149] *ibid*. section D.

[150] *ibid*. section C(20).

[151] For a full list of national eID means, see PBLQ, International Comparison eID Means (Final report, version 1,0, 10 April 2015) <https://kennisopenbaarbestuur.nl/rapporten-publicaties/international-comparison-eid-means/> accessed 26 April 2018, 14-18.

[152] Countries like the UK and Denmark have opted for exclusively private-sector eID operators (due in part to the lack of governmental ID cards). See also recent decision of Italy to notify an eID led by the private sector: 'First private sector eID scheme pre-notified by Italy under eIDAS' (*European Commission*, 7 December 2017) <https://ec.europa.eu/digital-single-market/en/news/first-private-sector-eid-scheme-pre-notified-italy-under-eidas> accessed 26 April 2018.

[153] Government Digital Service, *Gov.UK Verify Data Protection Impact Assessment* (n. 44) 14.

[154] *ibid*.

then seem problematic to only rely upon entirely one-sided LOA.

From the analysis of the doctrine of legal basis as it can be derived from the GDPR it appears that the role given to consent has expressly been circumscribed in comparison with the DPD. As a result, it is arguable whether consent could be used at all to legitimise the processing of personal data for identification and authentication purposes in the context of the functioning of Gov.UK Verify. Furthermore, as it will be argued below, the characterisation of a situation of joint controllership should have implications for the choice of the appropriate legal basis.

4. Choosing the appropriate legal basis in a situation of joint controllership

After having unfolded the doctrine of joint controllership, distinguished it from a processor-controller relationship, and then checked to what extent eIDAS frames the relationships of the different parties to an eID scheme, the ecosystem of Gov.Uk Verify is assessed in light of these considerations.

4.1. *The doctrine of joint controllership*

The DPD does expressly acknowledge the possibility of having situations of joint controllership. It uses the expression *"alone or jointly with others"* and provides in its Article 2(d) that a data controller is

> *the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.*

The Article 29 Working Party in its opinion on the concepts of 'controller' and 'processor'[155] aims at providing guidance on the concept of 'alone or jointly with others' and refers back to the opinion of the Commission on the European Parliament to explain that a situation of joint controllership can exist even in situations in which the data controllers do not *"equally"* determine the means and purposes of a *"single processing operation."*[156]

The Article 29 Working Party confirms that the same approach as the approach to be used for the characterisation of a situation of sole controllership is relevant: *"a substantive and functional approach,… focusing on whether the purposes and means are determined by more than one party."* [157]

Whereas the Article 29 Working Party seems at the start of its analysis to consider that each data controller shall contribute to both the determination of the means and the purposes of the processes, it modifies its analysis and adds a few lines later that it suffices for the data controller to determine either the purpose or the essential elements of the means:

> *In this perspective, joint control will arise when different parties determine with regard to specific processing operations either the purpose or those essential elements of the means which characterize a controller.*[158]

In other words, a data processor should be considered a joint controller if it determines the purpose or the *"essential elements"* of the means that characterize a controller.[159] A large variety of situations of joint controllership could thus be found.[160] This is the case in particular when *"different actors would decide to set up a shared infrastructure to pursue their own individual purposes."* [161] Such an approach makes particular sense in cases in which there is a significant asymmetry of information between the party taking the initiative of the processing and the party developing the means.

The Article 29 Working Party goes on to distinguish between two complementary approaches that are both relevant in order to determine whether one is faced with a situation of joint controllership: a micro-level approach and a macro-level approach. In the words of the Article 29 Working Party:

> *In some cases, various actors process the same personal data in a sequence. In these cases, it is likely that at micro-level the different processing operations of the chain appear as disconnected, as each of them may have a different purpose. However, it is necessary to double check whether at macro-level these processing operations should not be considered as a "set of operations" pursuing a joint purpose or using jointly defined means.*[162]

In a chain of processing activities, the pursuance of a 'joint purpose' thus appears crucial for the characterisation of a situation of joint controllership. And it is the characterisation of this joint purpose that should explain why under GDPR Article 82 joint controllers *"are involved in the same processing"* which would therefore lead to joint and several liability.

As an interesting point of reference, a typology of the various different types of relationships between data controllers, co-controllers, and processors, developed in 2005 by Olsen and Mahler, encompasses the majority of the types of collaboration envisaged by the Article 29 Working Party in its guidance.[163] Particularly, it was identified that joint controllers could come in two forms: partly joint controllers and fully scope joint controllers. A partly joint controller would be

[155] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169, 16 February 2010).
[156] *ibid*. 18.
[157] *ibid*. 18.
[158] *ibid*. 19.
[159] As has been noted elsewhere, however, the Working Party's distinction between 'essential' and 'non-essential' means appears to conflict with the definition of 'controller' found in Article 2(d) of the DPD. See Patrick Van Eecke and Maarten Truyens, 'Privacy and social networks' (2010) 26 Computer Law & Security Review 535, 539.
[160] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (n. 155) 19.
[161] *ibid*. 19.
[162] *ibid* 20.
[163] Thomas Olsen and Tobias Mahler, Privacy - Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems (LEGAL IST: Legal Issues for the Advancement of Information Society Technologies, Deliverable D11, 2005), 40-47.

present where the purpose and means of a certain processing operation is determined jointly by more than one controller, while others are performed separately under the sole control of another controller. A controller could be considered a full-scope joint controller if it and another controller jointly determine all the purposes and means of a particular data processing operation.[164]

Interestingly, the Article 29 Working Party directly mentions the example of e-government portals, which are described as falling within the category of joint controllership. This is because *"various actors involved jointly determine,* [even if it is to a different extent]*, the purposes and/or the means of a processing operation."* [165] It is worth repeating the Article 29 Working Party's explanation in detail:

> *E-Government portals act as intermediaries between the citizens and the public administration units: the portal transfers the requests of the citizens and deposits the documents of the public administration unit until these are recalled by the citizen. Each public administration unit remains controller of the data processed for its own purposes. Nevertheless, the portal itself may be also considered controller. Indeed, it processes (i.e. collects and transfers to the competent unit) the requests of the citizens as well as the public documents (i.e. stores them and regulates any access to them, such as the download by the citizens) for further purposes (facilitation of e-Government services) than those for which the data are initially processed by each public administration unit. These controllers, among other obligations, will have to ensure that the system to transfer personal data from the user to the public administration's system is secure, since at a macro-level this transfer is an essential part of the set of processing operations carried out through the portal.*

Although this explanation was written in 2010, when Gov.UK Verify was not even in its infancy and most the existing eID schemes were centralised and run by public authorities,[166] this does not necessarily mean that the analysis has to be different when the eID scheme at stake is conceived as a federated system, even if a distinction should be drawn between the eID means as such and other types of personal data processed by government services.

Of importance for the characterisation of a situation of joint controllership is also the observation that it is not conclusive that one data controller is not in a position to meet all the obligations of a data controller and that one data controller within the team is better placed to perform certain data controller obligations.[167] Furthermore, the Article 29 Working Party insists that the lack of transparency as regards the allocation of roles between the different data controllers can lead to an infringement of the principle of fair processing.[168] This is a position that has been implicitly endorsed by the UK ICO.[169]

The GDPR goes further than the DPD: not only is the GDPR more explicit in its recognition of situations of joint controllership, but also it expressly derives the consequences of such a characterisation in terms of liability. For the moment suffice to say that the GDPR imposes an obligation for joint data controllers to determine in a transparent manner their roles and responsibilities in the light of the GDPR in order to ensure compliance, in particular compliance with data subject rights such as the right to information, *"unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject."*[170] This is repeated in the Article 29 Working Party's recent Guidelines on transparency.[171]

With this said, the choice between a characterisation of a situation of joint controllership and a processor-controller relationship is not necessarily a straightforward exercise. After having recalled the two cumulative criteria for qualifying an actor involved in the processing of personal data a processor that originates from DPD Article 2(e),[172] *i.e.* being an entity separate from the controller and processing personal data on behalf of the controller, the Article 29 Working Party offers a bundle of indicators to identify a processor-controller relationship:

- The range of the margin of manoeuvre left to the processor as a result of the instructions of the controller.
- The modalities of the monitoring undertaken by the controller to supervise the activity of the processor.
- The information provided by the controller to data subjects in relation to the allocation of roles between the different parties and thereby the expectations of data subjects as a consequence of this information.
- The degree of expertise of each party.[173]

However, the Article 29 Working Party insists upon the complexity of processing activities, which can lead to prefer the characterisation of a situation of a joint data controllership rather than a processor-controller relationship when combined with an assessment of the privacy risks:

---

[164] *ibid*. This clarification aside, however, some observers have suggested that the notion of joint controllership remains a vague and confusing concept, particularly in certain contexts. See e.g. Jenna Mäkinen, 'Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things' (2015) 24 Information & Communications Technology Law 262, 262-277.

[165] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (n. 155), 21.

[166] In its 2011 report, the OECD notes that out of the 16 countries examined, 12 were operating centralised registration eID policies: OECD, Digital Identity Management: Enabling Innovation and Trust in the Internet Economy (2011) <http://www.oecd.org/sti/ieconomy/49338380.pdf> accessed 26 April 2018, 44.

[167] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (n. 155) 22.

[168] *ibid*. 24.

[169] See ICO, *The Guide to Data Protection* (n. 86) 8-9; ICO, Data Controllers and Data Processors: What the Difference is and What the Governance Implications Are (Guidance, 06 May 2014) <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> accessed 26 April 2018, 6.

[170] GDPR Art. 26(1).

[171] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679 (WP 260 rev 01, adopted on 29 November 2017, as last revised and adopted on 11 April 2018), at para. 44.

[172] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (n. 155) 25.

[173] *ibid*. 28.

> *the complexity of processing operations may lead to put more focus on the margin of manoeuvre of those entrusted with the processing of personal data, e.g. when the processing entails a specific privacy risk. Introducing new means of processing may lead to favouring the qualification as data controller rather than data processor. These cases may also lead to a clarification – and appointment of the controller – explicitly provided for by law.*[174]

Taking the example of processing activities undertaken for historical, scientific and statistical purposes, including anonymisation practices, the Article 29 Working Party specifies that when data coming from different sources are combined together, *"there is a particular threat to data protection, justifying the intermediary organization's own responsibility."*[175]

Notably, in his opinion delivered in *Facebook Ireland*,[176] AG Bot endorses the Article 29 Working Party's functional approach to controllership and interpreting the DPD (Article 2(d)) qualifies the operator of a Facebook fan page as a joint controller, even if Facebook is described as principally deciding *"upon the purposes and means of the processing."* [177] AG Bot clearly states:

> *no distinction should be made, in my opinion, between an undertaking which equips its website with tools similar to those offered by Facebook and an undertaking which joins the Facebook social network so as to benefit from the tools which Facebook offers.*[178]

Because with the GDPR, the demarcation between the roles of processor and controller becomes less clear as processor obligations have been multiplied and the status of processor made closer to that of controller, one could make the argument that the balance should be tipped in favour of a characterisation of a situation of joint controllership.[179]

That joint controllers should be considered to be joint and severally liable is a not a novelty of the GDPR. Despite the silence of the DPD, the Article 29 Working Party had interpreted the DPD in 2010 as implying that the default rule under the DPD was that of joint and several liability.[180] However, the GDPR offers a more radical solution than the one anticipated by the Article 29 Working Party. This is because even when joint controllers determine in a transparent manner their roles and responsibilities for the purposes of ensuring compliance with the GDPR, joint data controllers remain jointly and severally liable. GDPR Article 26(3) provides that: *"Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers."* Reading Article 26(3) together with Article 82 it appears that one joint controller will only be able to escape liability for the actions of another if it can demonstrate that *"it is not in any way responsible for the event giving rise to the damage"*.[181]

4.2. *eIDAS partition of roles*

As hinted above, eIDAS identifies the main actors of an eID scheme and their roles in the process of identification and authentication. However, and this is very important, eIDAS adopts a technologically neutral approach and does not aim to dictate the way eID schemes should be designed.[182] Besides, observing the various eID schemes that have been deployed by Member States, there is a great variety of architectures. This has been recognised during the preliminary work leading to eIDAS. In 2013 a feasibility study conducted as part of the EU IAS project noted that eID *solutions "were heterogeneous from a technology perspective, using smartcards* […], *Mobile eID's* […], *allowing soft certificates* […], *or even username/password* […]." [183] It continued that "[m]*ost solutions were established well before there was a common middleware standard"* [184] which forced the STORK pilot (upon which eIDAS builds) *"to create a model that could accommodate the various existing models."* [185] Along the same lines, the impact assessment accompanying the eIDAS proposal acknowledged as a problem that *"Member States use different technological solutions for personal identification which lead to interoperability problems when it comes to cross-border interaction."*[186] eIDAS aims at supporting the creation of an interoperability framework to make cross-border transactions possible, and its implementation acts to some extent constrain its design.[187] However, per definition this is true only in the context

---

[174] *ibid*. 29.
[175] *ibid*. 30.
[176] Opinion of Advocate General Bot in *Wirtschaftsakademie Schleswig-Holstein*, Case C-210/16, [2017] (EU:C:2017:796).
[177] *ibid*. 47.
[178] *ibid*. 64.
[179] This is a proposition that has been alluded to in the data protection literature, with some observers suggesting that the blurring of boundaries between data controllers and data processors caused by technological evolution could lead to the emergence of a 'confused' approach to data protection. See for example Peter Blume, 'Controller and processor: is there a risk of confusion?' (2013) 3 International Data Privacy Law 140, 140-145. See also W. Kuan Hon, Christopher Millard and Ian Walden, 'Who is responsible for 'personal data' in cloud computing?—The cloud of unknowing, Part 2' (2012) 2 International Data Privacy Law 3, 3-18.
[180] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (n. 155) 22.
[181] GDPR Art. 82(3).
[182] eIDAS Art. 12(3)(a) provides that the interoperability framework aims *"to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State."*
[183] European Commission, Feasibility study on an electronic identification, authentication and signature policy (IAS) (Final Version (D11b), Ref Ares(2013)2869715, 13 August 2013) <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2794> accessed 26 April 2018, 171.
[184] *ibid*. 172.
[185] *ibid*.
[186] European Commission, Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (COM(2012) 238 final, 4 June 2012) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0136&from=EN> accessed 26 April 2018, 10.
[187] There have been arguments against the requirement of a Minimum Dataset (Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance) [2015] OJ L 235/1, ANNEX) as well as a technical specification that would best serve central deployments and does not lend itself to newer technologies, such as zero-knowledge-credentials. See for example ABC4Trust Position Paper,

of cross-border transactions and not in the context of domestic transactions. This is because the interoperability framework has been conceived as a means to identify a minimum common denominator that could be accepted by all Member States without affecting the design and development of their eID schemes when used for internal transactions. As a result, eIDAS shall not be seen as determining in a comprehensive way the respective roles and responsibilities of controllers involved in national eID schemes.

What is true, nevertheless, is that eIDAS identifies two processing purposes: identification and authentication, which should (although this is not explained in these terms in eIDAS), comprise two stages: the creation of the eID means with person identification data and the subsequent use of the eID means for authentication purposes. eIDAS definitions are nevertheless slightly confusing, as they seem to overlap:

- Electronic identification: *"the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person."*[188]
- Authentication: *"electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed."*[189]

As a result, it is not entirely clear whether electronic identification only covers the creation of the eID means or subsequent acts of authentication. With this said, despite the imprecision of the language the creation of the eID means and the confirmation of the identity of an individual through the means of an eID means are closely related and are captured by either electronic identification or authentication, if not both.

As aforementioned, eIDAS distinguishes between three actors: notifying Member States, parties issuing eID means and parties operating authentication procedures. eIDAS expressly recognises the fact that eID means can be issued by private parties. eIDAS Article 7 therefore distinguishes between three hypotheses: when the eID means are issued by the notifying Member State, under a mandate from the notifying Member State, or independently of the notifying Member State but are recognised by that Member State.

The notifying Member State appears to be the one with the most obligations or duties. It shall ensure:

- *The person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued.*[190]
- *The availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form.*[191]
- *The cross-border authentication [is] provided free of charge when it is carried out in relation to a service online provided by a public sector body.*[192]

Strangely, parties operating authentication procedures do not seem to be subject to any specific obligation or duty.

Parties issuing eID means shall ensure:

- *The electronic identification means is attributed to the person referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3).*[193]

The afore description confirms that the obligations and duties of eIDAS actors are broadly formulated and not necessarily data protection related but do cover personal data processing activities. In this sense, the domain *rationae materiae* of eIDAS seems broader in scope than the domain of the GDPR. At the same time, eIDAS is narrower in scope (*rationae personae*) than the GDPR in that it only targets three types of actors. As eIDAS makes compliance with EU data protection law a requirement for both electronic identification and trust services as per Article 5, there is no reason why the key tenets of EU data protection should not be applied in this context and in particular the doctrine of joint controllership, although this raises question of compatibility between GDPR Article 26 and 82 and eIDAS Article 11.

4.3. *Gov.UK Verify and its segregation of roles and responsibilities*

The Verify DPIA attempts to distinguish between two types of purposes in order to then distinguish the processing activities of Identity Providers-Certified Companies from the processing activities of GDS. It is explained that *"GDS will process personal data for the purpose of matching Service Users to Government Service records."*[194] At the same time, *"[p]urposes for Certified Companies processing personal data are defined within the procurement documentation, and Certified Companies are obliged to clearly state purposes in their privacy notices."*[195] This seems to explain or justify why Identity Providers and GDS are both data controllers. Yet, for their respective processing activities, a distinct legal basis is identified.

Privacy-ABCs and the eID Regulation (2014) <https://abc4trust.eu/download/documents/ABC4Trust-eID-Regulation.pdf> accessed 26 April 2018, 2; Fabio Massacci and Olga Gadyatskaya, How to get better EID and Trust Services by leveraging eIDAS legislation on EU funded research results (White Paper, October 2013, 2013) <http://www.cspforum.eu/Seccord_eidas_whitepaper_2013.pdf> accessed 26 April 2018, 3-4; Harald Zwingelberg and Jan Schallaböck, H2.4 The Proposal for a Regulation on Electronic Identification and Trust Services under a Privacy and ABC4Trust Perspective (Opinion Paper, ABC4Trust EU Project, 31 October 2013) <https://abc4trust.eu/index.php/pub/deliverables/176-h2-4> accessed 26 April 2018, 9-10.

[188] eIDAS Art. 3(1).

[189] eIDAS Art. 3(5).

[190] eIDAS Art. 7(d).

[191] eIDAS Art. 7(f).

[192] eIDAS Art. 7(f).

[193] eIDAS Art. 7(e).

[194] Government Digital Service, *Gov.UK Verify Data Protection Impact Assessment* (n. 44) 24.

[195] *ibid.* 24-25.

A careful analysis of both the Framework Agreement and the reality of the practices show that the different processing activities are better described as a set of processing activities aimed at a common purpose: authentication.

While contractual arrangements are a useful tool to characterise the situation at hand, this does not mean that the qualifications retained by the parties should necessarily remain. These qualifications should be confronted with the factual arrangement of the relationship.[196]

The Framework Agreement, as aforementioned, specifies the purposes for the processing in its schedule 2(a) on services description to

> *provide the following online identity assurance services to users seeking to access any HMG Service, with the objective of allowing them to prove that they are who they claim to be to defined levels of assurance.*[197]

From the perspective of Service Users, *i.e.* data subjects, it would thus appear artificial to distinguish between the processing undertaken by Identity Providers, GDS and (government) Service Providers. The three types of processing activities aim to ensure the realisation of one process: authentication for communicating with a (government) Service Provider. It is therefore suggested that they should be conceived as a set of processing activities pursuing one joint purpose.

The question is then whether for this set of processing activities Identity Providers should be qualified as processors or data controllers. Under the Framework Agreement Identity Providers are imposed security obligations,[198] obligations to ensure data subjects can exercise their rights,[199] reporting obligations in favour of GDS,[200] obligation to request authorisation for the transfer of personal data to third countries,[201] to appoint any material sub-contractor,[202] obligations relating to the training of Identity Providers' personnel.[203] A monitoring and supervision mechanism is put in place.[204] Besides, GDS is meant to review each Certified Company's privacy notice.[205]

As the Verify DPIA confirms it, the set of processing activities at stake is a set of complex processing activities requiring the processing of data coming from a variety of sources, some of which should be considered more sensitive than others, *e.g.* authentication credentials and transactional data. Identity Providers have a key role: they store authentication credentials and have access to citizen verification data, *i.e.* "*information about or from passports and driving licences* (…) *commonly used to obtain other forms of ID,*" [206] which is rightly described as being "*more sensitive than other attribute data.*" [207]

There is thus an argument that Identity Providers should be characterised as joint data controllers with GDS and (government) Service Providers for the set of processing activities ultimately leading to authentication. This is because the processing activities are complex, the privacy risks are potentially significant (in the sense that misuse of personal data could lead to financial implications for data subject depending upon which government service is at stake) and they determine (in the sense of being in control of) essential elements of the processing means. In this line, what is particularly troubling is that the Verify DPIA does not attempt to assess the impact of the misuse of the Matching Dataset, not as regards the information contained within the Matching Dataset as such which is considered of a relatively low risk because it is publicly available, but as regards the information to which an attacker could gain access once having misused the eID means. Notably, the recent guidance of the ICO list 'federated identity assurance services' within the list of high risk processing.[208]

Assuming Gov.UK Verify embeds a situation of joint controllership between three parties: the Identity Providers, GDS and the (government) Service Providers, it then becomes problematic to exclude the activities of Identify Providers or Certified Companies from the scope of the compliance checks,[209] in particular if tScheme is not able to finalise the certification until an Identity Provider is actually operating. Yet, this is what happened when the first version of the Verify DPIA was performed.

More importantly, assuming Gov.UK Verify embeds a situation of joint controllership between the Identity Providers, GDS and the government Service Providers, the identification of a distinct legal basis for the processing performed by Identity Providers arguably becomes a moot point from the perspective of the data subjects or maybe more simply misleading. The same holds true if Identity Providers are only processors. Indeed, it is suggested in this paper that in order to identify the appropriate legal basis the set of processing operations should be considered as a whole. As a result, the most appropriate legal bases for identification and authentication purposes in the context of the functioning of Gov.Uk Verify, *i.e.* in order to access government services, should be performance of a task carried out in the public interest or the pursuance of a legitimate interest. It is suggested that a narrow interpretation of the former ground is however preferable from a data subject standpoint.

Finally, assuming Gov.UK Verify embeds a situation of joint controllership, this would require revising the allocation of responsibilities between the different parties, despite the fact

---

196 Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (n. 155) 18.

197 Cabinet Office, *Framework Agreement and Schedules* (n. 27), sch. 2 (part 2(A1)). See also clause 13.1.

198 *ibid*. clause 17.4.

199 *ibid*. clause 17.4.

200 *ibid*. clause 17.5.

201 *ibid*. clause 17.6.

202 *ibid*. section F(23).

203 *ibid*. section F(22).

204 *ibid*. section E(20).

205 Government Digital Service, *Gov.UK Verify Data Protection Impact Assessment* (n. 44) 11.

206 *ibid*. 19.

207 *ibid*. 19.

208 ICO, Guide to the General Data Protection Regulation - Data Protection Impact Assessments (DPIAs) (v.22 March 2018 - 1.0.77) <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf> accessed 26 April 2016.

209 *ibid*. 23. The reason given is that these companies are covered by separate contractual and legal obligations.

that eIDAS expressly contains a provision on liability in its electronic identification chapter, *i.e.* Article 11.[210] Indeed as aforementioned the GDPR opts for a principle of joint and several liability in its Article 82(4–5) to be read together with Article 26(3), which seems to be incompatible with eIDAS Article 11, premised on the principle of several liability.

5. Conclusion

To conclude, this article suggests that due to the way in which the GDPR strengthens both the rights of data subjects (*e.g.* through granting a right to compensation based upon a presumption of liability), and revisits the status of data controllers and data processors as well as narrows down the remit of the legal basis based on consent, it should have a significant impact in the field of electronic identification as in many other sectors. One conclusion that can be drawn from this observation is, therefore, that data protection impact assessments performed at the time of the DPD should be reconducted in order to take fully into account the novelties brought about by the GDPR. Critically, the Verify DPIA conducted for the purposes of establishing GOV.UK Verify should be conducted afresh, as its development to date has seemingly been premised upon a DPIA that is now worryingly outdated, and as matter of urgency, to engineer data protection principles as early as possible. As a means of supporting this position, this article has highlighted and analysed several apparent flaws in the Verify DPIA, the most significant and notable of which being the identification of an erroneous selection of legal bases. In addition, the set of liability stipulations would also appear to be incompatible with the substantive provisions of the GDPR and in particular its Article 82.

More specifically, the article has argued that identifying the appropriate legal basis for the processing of personal data requires a prior understanding and characterisation of the relationship between the different actors. This is because, given the involvement of stronger parties, such as public authorities, it may be that some legal bases should be excluded from the very beginning. Furthermore, it is suggested that the characterisation of a situation of joint controllership as much as a processor-controller relationship requires taking a holistic approach to the set of processing activities intended to achieve a specified and/or specific purpose. The foregoing is to ensure data subjects' expectations are taken into account and to guarantee the full effects of Article 82 of the GDPR. In the context of GOV.UK Verify this would mean that one legal basis should ground the processing of three actors: the Identity Providers, GDS and the (government) Service Providers, which should be characterised as joint controllers. This should have implications for both the scope and content of the next version of the Verify DPIA, assuming GOV.UK Verify is pushed forward even if it is further privatised, as well for data subject rights in general, such as the right to compensation.

Acknowledgement

This research was funded by the Research Councils UK Digital Economy Programme, Web Science Doctoral Training Centre, University of Southampton, EP/L016117/1, and the European Union's Horizon 2020 research and innovation programme under grant agreement No 700542. This paper reflects only the authors' views; the Commission is not responsible for any use that may be made of the information it contains.

The authors would like to thank Mark King (a member of EEMA) for drawing their attention to some relevant details. All errors are our own.

[210] eIDAS Article 11 could be seen to be in conflict with GDPR Article 82 as there is no presumption of liability.