CLOUD ACCOUNTABILITY PROJECT

D:D-4.1 The Rise of Compliance Audits - Cloud Investigations by European Data Protection Authorities: An Empirical View

Deliverable Number:	D44.1a
Work Package:	WP 44
Version:	Final
Deliverable Lead Organisation:	QMUL
Dissemination Level:	PU
Contractual Date of Delivery (release):	28 February 2015
Date of Delivery:	28 February 2015

Editor

Asma Vranaki (QMUL)

Contributors

Asma Vranaki (QMUL), Chris Reed (QMUL)

Reviewers

Dimitra Stefanatou (TiU), Karin Bernsmed (SINTEF)

Executive Summary

This deliverable presents the qualitative empirical findings of T:D-4.1 of Work Package 44 of the Cloud Accountability Project. This exploratory deliverable draws on qualitative interviews, documentary analysis and observation data to analyse how and why European data protection authorities ('EU DPAs') exercise one of their statutory enforcement powers, namely, investigations more frequently to determine the compliance of cloud providers with the relevant data protection laws. This deliverable presents four arguments. Firstly, regulating Cloud Providers through investigations is a complex process which involves different relationships of co-operation between various actors, such as DPAs operating under distinct data protection laws. In practice, manifold interactions and practices, such as facilitative instruments, are deployed to form and perform such collaborative tasks which are significant to ensure the consistent application and enforcement of common data protection principles (derived from distinct in an increasingly globalised context. Moreover, complexity can also manifest itself through several factors, such as budgetary constraints and pressures from stakeholders including the press, which impact on key aspects of Cloud Investigations. How such complexities are resolved during Cloud Investigations can often involve intricate and context-specific strategies, such as delegating action to a third-party. Secondly, regulation through Cloud Investigation is dynamic as it is a process which involves constant activities from multiple actors. In particular, Cloud Investigations can involve constantly evolving regulatory styles (e.g. from soft to hard to soft) and compliance attitudes which mean that the regulatory encounters between Cloud Providers and EU DPAs during an investigation often involve ceaseless change. Thirdly, Cloud Investigations can, at times, be contested as EU DPAs and Cloud Providers attempt to resist each other`s attempts to direct the investigation in particular ways. Finally, we argue that many reasons including the benefits of rapport-building, and relocation of some of the operations of multinational Cloud Providers to Europe, can account for why Cloud Investigations are growing in frequency in Europe. Here we also underline how the construction of specific realities during some Cloud Investigations (e.g. compliance attitudes) can hamper the effectiveness of Cloud Investigations as regulatory tools in the sense of enforcing all the relevant data protection laws.

Table of Contents

1 Introduction

This deliverable,[1] D-4.11, forms part of the stream of work under T:D-4.1 of Work Package 44, entitled 'D-4: Contracts, SLAs, and Remediation' ('D4'), of the Cloud Accountability Project ('A4 Cloud').[2]

As detailed, in the preliminary D-4.11, in early 2014, T: D-4.1 was amended, with the relevant approvals, because one of the main outputs of D4, the Cloud Offerings Advisory Tool, was modified.[3] The new stream of work under T: D-4.1 is being undertaken by using socio-legal research methods and concepts[4] in order to shed light on how European data protection authorities ('EU DPAs') regulate 'personal data' by deploying one specific regulatory tool,[5] namely, investigations,[6] in the context of cloud computing. EU DPAs are the statutory independent[7] public regulatory bodies which have various functions including

[1] We would like to thank Clémentine Carlet, Lou Matas, István Fancsik, Giuseppina Claudia Coniglione and Dr Niamh Gleeson of QMUL for assisting us in researching the data protection laws of various European member states. As all our interviews were conducted on a non-attributable basis, we cannot identify the European member states in question.

[2] A4 Cloud, Description of Works for Work Package 44 (as amended in August 2014), 1ff.

[3] Asma Vranaki and Chris Reed, 'The Rise of Investigations by European Data Protection Authorities in the Context of Cloud Computing,' (A4 Cloud, WP 44, D-4.11, 30 September 2014).

[4] Socio-legal studies refers to the study of law in context. For more on socio-legal research methods and concepts see Denis Galligan, *Law in Modern Society* (Oxford University Press 2007) and Roger Cotterrell, *Law's Community: Legal Theory in Sociological Perspective*, (Oxford Socio-Legal Studies Clarendon Press, 1997).

[5] For more on links between 'regulatory tools' and technology, see R Brownsword and K Yeung, 'Regulating Technologies: Tools, Targets and Thematics' in Brownsword R and Yeung K, (eds) Regulating technologies: legal futures, regulatory frames and technological fixes (Hart 2008) 3.

[6] For more on investigations as regulatory tools in the data protection arena, see P Carey, *Data Protection: A Practical Guide to UK and EU Law* (OUP 2011) 69 and 127; Philip Schütz, 'The Set Up of Data Protection Authorities as a New Regulatory Approach,' in S Gutwirth et al *European Data Protection: In Good Health?* (Springer Netherlands 2012) 125. See n 10.

[7] For more on EU DPAs` independence from the influence of government, legislature and other stakeholders, see Lee A Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002). See Article 28 of the 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 L281/31 ('DPD') for more on the powers of European DPAs.

applying and enforcing data protection laws in European member states.[8] Investigations refer to the one of the enforcement powers of EU DPAs, namely, their power to investigate 'data controllers'[9], such as companies which offer cloud computing services or technologies ('Cloud Providers'), in specific circumstances (e.g. when an individual complains).[10] 'Personal data' mean 'any information relating to an identified or identifiable natural person.'[11]

One of the formal deliverable produced by the amended T: D-4.1 is this D-4.11. We submitted a preliminary version of D-4.11 on 30 September 2014 which examined some of our empirical findings, such as how the investigations of Cloud Providers by EU DPAs ('Cloud Investigations') have multiple and context-specific aims (e.g. educating Cloud Providers) and are deployed through manifold methods (e.g. questionnaire, and technical testing) and practices (e.g. discussions, negotiations, and explanations).[12] In this consolidated version of D-4.11, we analyse the empirical findings which have not been examined in the preliminary D-4.11.

[8] In different jurisdictions, various labels are used to denote the statutory independent public regulatory body which has the function of applying and enforcing data protection laws. For example, in the UK the DPA is referred to as the 'Information Commissioner' where as in Italy the DPA is referred to as 'Il Garante per la protezione dei dati personali.'Additionally, in some legislative frameworks (E.g. DPD, ibid) and scholarly articles (e.g. Colin J Bennett, 'International Privacy Standards: can Accountability be Adequate?' (2010) 106 Privacy Laws and Business International 21), other terms including supervisory authorities and privacy commissioners are used to refer to such bodies. In this deliverable, we refer to such bodies as data protection authorities ('DPAs'). It should be noted that other regulatory institutions, such as the national courts, can also be involved in enforcing data protection laws. For example, many national courts have the power to hear appeals from enforcement decisions taken by DPAs. For more see Bygrave (n 7).

[9] Article 2(d) of the DPD (n7) defines the 'data controller' as a '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.'

[10] Article 28(3), DPD (n7). It should be noted that Article 28 has been inconsistently transposed by various European member states. For more on this, see Bygrave (n 7), 71ff.

[11] Article 2(a), DPD (n 7)

[12] n 7.

1.1 Cloud Computing, Data Protection, and Investigations by Data Protection Authorities

In recent years, the societal and economic benefits of cloud computing have been increasingly recognised by various stakeholders.[13] Cloud computing is a vague and wide term.[14] In essence, it refers to the delivery of computing resources (e.g. data storage, communication, and network) as a service through a network (e.g. the internet) on a scalable and on-demand basis.[15] Numerous industry quantitative research have underlined the increasing uptake of cloud-based services globally[16] including Europe.[17] As businesses[18] and

[13] E.g. Commission, 'Unleashing the Potential of Cloud Computing in Europe' COM (2012) 529 final.

[14] E.g. For more on the different meanings of cloud computing see, Luis M Vaquero,et al, 'A break in the clouds: towards a cloud definition,' (2008) 39(1) ACM SIGCOMM Computer Communication Review 50, Michael Armbrust et al, 'A view of cloud computing,' (2010) 53(4) Communications of the ACM 50. Moreover, there is considerable debate about whether cloud computing is a 'new dawn' or 'just another day'. For example, in a 2009 interview, Larry Ellison, the Chief Executive Officer of Oracle, opines that 'all the cloud is, is computers in a network…Our industry is so bizarre. I mean, they just change a term and think they've invented technology.' <http://www.youtube.com/watch?v=KmXJSeMaoTY> from Cloud U, 'Revolution not Evolution: How Cloud Computing Differs from Traditional IT and Why it Matters,' (2011) < http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Revolution_Not_Evolution-Whitepaper.pdf> accessed 10 February 2015. However, Marc Benioff of the Salesforce fervently countered Ellison`s views on cloud computing at the Oracle OpenWorld Conference 2010: 'Our definition of Cloud Computing is multi-tenant, it's faster, half the cost, pay as you go, it grows as you grow or shrinks as you shrink. It is extremely efficient. We're not going to show you computers taller than you. We're not going to show you a cloud in a box because clouds don't come in a box. They never have. That's the whole idea.' See 'Benioff fires back at Oracle's Ellison,' (CRB Online 22 September 2010) <http://www.cbronline.com/blogs/cbr-rolling-blog/salesforcecom-fires-back-at-oracles-ellison-benioff-oracle-openworld-220910> accessed 10 February 2015.

[15] For more, see W Kuan Hon and Christopher Millard, 'Cloud Technologies and Services,' in (eds) Christopher Millard, *Cloud Computing Law* (Oxford University Press 2013) 1.

[16] For example, on 26 February 2015, Tata Communications published the findings of an independent research project on cloud computing. The findings of the research was based on 1,000 interviews of senior IT decision-makers in private organisations with 500+ employees. Interviews were conducted in eight countries (e.g. UK, France, China, and India) and the respondents worked in a wide range of industry sectors (e.g. IT; retail, distribution, and transport; business and professional services). Consequently, despite Tata Communications` vested interest in the research project, the research findings meet the criteria of validity (e.g. findings that go against Tata Communications` interests, such as the finding that 57% of respondents said that their organisation has migrated data back in-house due to data protection and security concerns and are relying mostly of private clouds) as well as provide an in-depth and broad snapshot of the uptake of cloud computing in key jurisdictions. According to this research, 97% of the respondents said that their organisations had already adopted cloud computing to some extent and 84% of respondents said that cloud computing was already critical or very important to their business.

consumers embrace innovative cloud services and technologies, there are growing concerns about the data protection and privacy issues raised by such technologies.[19] For example, as cloud computing often involves a complex supply chain where more than one Cloud Provider can be involved in delivering a service, it can be difficult to ascertain which Cloud Providers are acting as data controllers or 'data processors.'[20] Evidently, this is key in determining the obligations of such cloud providers under national data protection laws.[21] Consequently, in various jurisdictions, the the data processing operations and policies of popular Cloud Providers, such as Facebook, and Google are being more frequently scrutinised by

---

[17] A recent research by the European Commission has estimated that cloud computing could contribute up to €250 Billion to the European GDP in 2020 and 3.8 Million jobs. See C et al Bradshaw, Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake, (IDC Research Report, July 2012) < http://www.icon-project.eu%2Fdocs%2Fupload%2F201310%2FCloud-Computing.pdf&ei=55TtVKTfHZLOaKqkgoAL&usg=AFQjCNG0Y_sgKVs-Vs-cFstuQvT_y7Mkog&sig2=Lze7JjH1532krz92UZlbGg> accessed 10 February 2015.

[18] Examples of recent adoption of cloud-based solutions by organisations operating in various sectors include the adoption of a multi-million pound cloud-based telecoms, network, contact centre and mobile contract solutions by the automotive organisation Scania UK [Business Cloud News, 'Scania drives its comms platform into the cloud,' (24 February 2015) < http://www.businesscloudnews.com/2015/02/24/scania-drives-its-comms-platform-into-the-cloud/> accessed 24 February 2015], the adoption of the Rackspace Managed Cloud Portfolio by the electronic commerce website Made-in-China.com ['Made-in-China.com Increases Website Traffic Over 2000 Percent With Rackspace,' (Rackspace Investor Relations 8 January 2015) < http://ir.rackspace.com/phoenix.zhtml?c=221673&p=irol-newsArticle&ID=2004956> accessed 10 February 2015], and the move of the e-commerce specialist, London Ferrett to the cloud to deal with increased traffic during Black Friday ['How one retailer managed to survive Black Friday with the cloud,' (Cloud Computing Intelligence 12 December 2014) < http://cloudcomputingintelligence.com/more-news-and-features/item/1719-how-one-retailer-managed-to-survive-black-friday-with-the-cloud> accessed 10 February 2015.

[19] E.g. see n 15. We do not engage in the conceptual differences between data protection and privacy in this deliverable. For more, see O Lynskey,' Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order,' (2014) 63(3) International and Comparative Law Quarterly, 63(03), 569.

[20] Article 2 (e) of the DPD (n 7) defines a data processor as 'a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller'; Article 29 Data Protection Working Party, Opinion 1/2010 on the Concepts of 'Controller' and 'Processor' controller" and "processor" (16 February 2010) < http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf> accessed 10 February 2015.

[21] E.g. In Ireland, section 2 of the Data Protection Act 1988 as amended in 2003 < http://www.lawreform.ie/_fileupload/RevisedActs/WithAnnotations/EN_ACT_1988_0025.PDF> accessed 10 February 2015. In the United Kingdom, section 4(4) of the Data Protection Act 1998 < http://www.legislation.gov.uk/ukpga/1998/29/section/4> accessed 10 February 2015.

regulators.[22] In Europe, various EU DPAs are starting to investigate several multinational Cloud Providers ('Cloud Investigations).[23] Thus, it becomes important to understand how and why personal data is regulated through such Cloud Investigations in Europe.[24]

This exploratory deliverable does not significantly engage with the relevant conceptual notions, such as, compliance attitudes,[25] but rather makes preliminary links between our empirical findings and the relevant analytical constructs, such as regulatory styles.[26] Nonetheless, the empirical findings analysed in this deliverable has been fully informed by the relevant data protection, privacy, and technology regulation literature.[27] In line with emerging literature, we have avoided adopting a 'tools-only' perspective when analysing how and why Cloud Investigations are deployed.[28] Such perspectives can be limited as they often focus solely on the regulatory tools without considering how multiple

[22] E.g. See n 23.

[23] E.g. A29WP, Google Privacy Policy: Main Findings and Recommendations (16 October 2012) < http://www.cnil.fr/fileadmin/documents/en/GOOGLE_PRIVACY_POLICY-_RECOMMENDATIONS-FINAL-EN.pdf> accessed 16 July 2014; Letter from A29WP to Google (16 October 2012) < http://dataprotection.ie/documents/press/Letter_from_the_Article_29_Working_Party_to_Google_in_relation_to_its_new_privacy_policy.pdf> accessed 16 July 2014; Office of the Privacy Commissioner of Canada and the College Bescherming Persoonsgegevens, 'WhatsApp`s violation of privacy law partly resolved after investigation by data protection authorities,' (Press Release 28 January 2013) < https://www.priv.gc.ca/media/nr-c/2013/nr-c_130128_e.asp> accessed 12 September 2014. See Section 3 of the preliminary D-4.11.

[24] E.g. Abraham Newman, *Protectors of Privacy: Regulating Personal Data in the Global Economy* (Ithaca NY Cornell University Press 2008).

[25] Compliance attitudes refer to how Cloud Providers respond to the regulatory tool of investigation by for example partly or fully complying with the recommendations of the EU DPA because of normative reasons (e.g. recognising its duty to comply with the law) or strategic reasons (e.g. calculated compliance to derive a specific benefit such as avoiding a lawsuit).

[26] Regulatory styles refer to approaches, techniques and strategies deployed by the EU DPA during a Cloud Investigation.

[27] E.g. n 7, 29, 24, 123, 149, Colin J Bennett, 'Privacy advocacy from the inside and the outside: Implications for the politics of personal data protection in networked societies,' (2011) 13(2) Journal of Comparative Policy Analysis 125, Colin J Bennett, *Regulating privacy: data protection and public policy in Europe and the United States* (Cornell University Press 1992).

[28] E.g. Lawrence Lessig, *Code Version 2.0* (Basic Books 2006).

actors interact with such tools and how such tools are enacted empirically.[29] Consequently, the 'tools-only' accounts often fail to examine the complex and dynamic ways in which multiple actors interact with each other and the 'tools' in practice. From a 'tools-only' viewpoint, regulation is conceived in simpler terms as a static and linear process which flows from only one direction (i.e. from the regulator to the regulatee). Our rich and in-depth empirical data highlights that regulation through Cloud Investigations is a fluid achievement which involves multiple and contingent factors, such as regulatory styles, resistance, compliance attitudes, facilitative instruments and more. Consequently, by analysing these manifold empirical actions and interactions we explore how Cloud Investigations are not merely a 'top-down' exercise of authority by the EU DPAs over the Cloud Providers.

1.2 Focussing on Cloud Investigations

The main objective of D-4.11 is to understand how and why the investigations of Cloud Providers by EU DPAs ('Cloud Investigations') are being deployed to regulate personal data. Through what methods, and practices are Cloud Investigations deployed? To what ends are Cloud Investigations triggered? What actors form and perform Cloud Investigations? What are the relationships between these actors during Cloud Investigations? What factors impact on Cloud Investigations (e.g. whether they are triggered, their scope, and their outcomes[30])?

1.3 Methods and Arguments

To explore these questions, we employed three main qualitative data collection methods, namely, documentary analysis;[31] observation;[32] and interviews of seven DPAs, four

---

[29] E.g. See Charles Raab and Paul de Hert, 'The Regulation of Technology: Policy Tools and Policy Actors,' in (ed) Karen Yeung and Roger Brownsword*, Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart 2008) 265ff.

[30] Outcome means whether the investigation succeeds in bringing the operations and policies of the Cloud Provider in line with the relevant data protection laws.

[31] Documents analysed included relevant data protection laws, such as, the DPD (n 7), relevant national data protection laws (e.g. Act No 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties, Wet bescherming persoonsgegevens, the Data Protection Act 1988 as amended in 2003), drafts of the proposed General Data Protection Regulation (i.e. Commission, 'Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM 2012 (011) final <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0011:en:NOT> ('Commission`s Draft'); Committee on Civil Liberties, Justice and Home Affairs, European Parliament (rapporteur: Jan Philipp

multinational Cloud Providers, and the representatives of two European institutions.[33] As we have explained our approach to documentary analysis and observation in the preliminary D-4.11, in this section we only examine how we tackled our qualitative interviews.

Interviewing was a suitable data collection method as it supplemented and consolidated our background knowledge (gained through observation and documentary analysis) as well as provided us with rich, complex, and detailed accounts of how and why Cloud Investigations are used to regulate personal data.[34] Between March and April 2014, we selected potential interviewees who would provide us with a detailed and broad cross-section of views on our research questions (section 1.2). Our initial analysis of relevant documents[35] and observation data[36] made clear that three categories of actors were relevant to our inquiry, namely, EU DPAs which have or are investigating Cloud Providers, Cloud

---

Albrecht), 'Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (2013) PE 501.927v05-00 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN>; and Council document 17831/13 <http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2017831%202013%20INIT> all accessed 10 February 2015) ('GDPR'); relevant press releases (e.g. Mark Zuckerberg, 'Our Commitment to the Facebook community,' (Facebook, 29 November 2011) < https://blog.facebook.com/blog.php?post=10150378701937131> accessed 1 July 2014.); reports published by DPAs following their Cloud Investigations (e.g. A29WP, Google Privacy Policy: Main Findings and Recommendations (16 October 2012) < http://www.cnil.fr/fileadmin/documents/en/GOOGLE_PRIVACY_POLICY-_RECOMMENDATIONS-FINAL-EN.pdf> accessed 16 July 2014; Section D of decision No. 2013-025 on 10 June 2013 by the Chair of the Commission Nationale de l`Informatique et des Libertes giving formal notice to the company Google Inc.; Dutch Data Protection Authority, 'Report on the Definitive Findings of the Investigation into the Processing of Personal Data for the WhatsApp Mobile Application by WhatsApp Inc,' (January 2013) <http://www.google.co.uk/url?sa=t&rct=j&q=WHATSAPP+DUTCH+DPA+REPORT&source=web&cd=2&ved=0CCsQFjAB&url=http%3A%2F%2Fwww.dutchdpa.nl%2Fdownloads_overig%2Frap_2013-whatsapp-dutchdpa-final-findings-en.pdf&ei=cdwSVPwJg-Zo0pKB6Ag&usg=AFQjCNFqJFjvUqFPWy3pZJwX6FdMJ9dxWQ&sig2=n2m10rQ6A1u13QolOL7skQ > accessed 12 September 2014.

[32] See Section 1.2, n 3.

[33] For more see, n 44- 46 below.

[34] For more on the merits of interviewing in generating rich and in-depth data whilst enabling the respondents to 'tell their story', see Mira Crouch and Heather McKenzie, 'The logic of small samples in interview-based qualitative research,' (2006) 45(4) Social Science Information 483.

[35] n 41.

[36] n 32.

Providers which have been or are being investigated by EU DPAs, and the representatives of European institutions which play key roles in discussing current and future European data protection laws. We identified over twenty[37] potential respondents from these three categories of actors by considering several factors including the investigative powers of EU DPAs, the administrative rules applicable to how some EU DPAs exercise their investigative powers, the EU DPAs` sizes, the Cloud Providers` offerings (e.g. single service or technology, suite of services or technologies, target market etc), the past or ongoing Cloud Investigations,[38] and the ease with which we could secure the participation of potential respondents.[39] Our sampling strategy enabled us to strategically interview respondents whose experiences were directly relevant to our research questions (e.g. as DPAs or Cloud Providers).[40]

Ethical approval was granted by the Research Ethics Committee of QMUL on 21 May 2014. Potential respondents were approached and informed of the nature and objectives of the study. Subsequently, the Principal Investigator conducted fourteen interviews over several days from May 2014 to December 2014 of the representatives of DPAs,[41] Cloud Providers,[42] and the European institutions.[43] We ensured that we reached

[37] There are no rules governing the minimum acceptable sampling size for qualitative interviews. For example, see C A B Warren, 'Qualitative Interviewing,' in J F Gubrium and J A Holstein (eds) *Handbook of Interview Research: Context and Method* (Thousand Oaks CA Sage, 2002) 99 suggests that 20-30 interviews support valid conclusions. However, Kathleen Gerson and Ruth Horowitz, 'Observation and interviewing: Options and choices in qualitative research,' (2002) *Qualitative research in action* 199, 223 argue that fewer than 60 interviews can be used to generate valid conclusions. The general rule of thumb is that the adequate number of qualitative interviews for a research project is always context-specific. The sample size should not be too small to prevent data saturation (e.g. recurrence of similar findings), theoretical saturation (e.g. multiple data sources supporting one conclusion) or informational redundancy. Additionally the sample size should not be too large so that the researcher is unable to understand the object of study in-depth. See Alan Bryman, *Social Research Methods* (OUP 2012) 425ff. In our present research project, between 10-20 interviews would provide a valid sample as Cloud Investigations in Europe are a recent phenomenon. Thus we target respondents whose activities are directly relevant to our research questions. For more on the virtues of a small sample (under twenty) see Crouch and Mackenzie (n 34).

[38] E.g. n 23.

[39] For more on sampling for qualitative interviews, see Nigel King and Christine Horrocks *Interviews in qualitative research* (Sage, 2010).

[40] For more on purposive sampling and its validity, see Bryman (n 37, 417 ff).

[41] Interview of the Commissioner of one EU DPA conducted by the Principal Investigator ('PI') on 30 May 2014 ('Interview 1'), interview of a senior official of another EU DPA conducted by the PI on 25

data (e.g. recurrence of similar findings) and theoretical (e.g. recurrence of findings which supports a theoretical notion) saturation.[44] Our respondents were senior representatives who were actively involved in Cloud Investigations. All the interviewed Cloud Providers were large multinational companies that have a sizeable market share in Europe. We targeted these organisations because, to date, they are the only types of Cloud Providers which have been investigated by EU DPAs.[45] Consequently, the empirical findings analysed in this deliverable are mostly relevant to the investigations of multinational Cloud Providers that have a strong European presence. However, our findings may also be of some relevance to small and medium Cloud Providers that may be investigated by EU DPAs. Specific aspects of the investigative process are likely to be similar in substance (e.g. aims, methods, and practices) although variable in scale (e.g. duration of investigation, extent of 'deep dive' etc).

All our interviews were conducted on a non-attributable basis over the telephone or by Skype depending on the respondents` availability. Consequently we are unable to provide any information, such as a list of the interviewed organisations, which identifies our respondents. On average the interviews lasted one hour. All interviews were audiotaped with the participants' consent and transcribed in full. We ensured that the transcribed interviews produced an accurate version of what the respondents said rather than a

July 2014 ('Interview 2'), interview of a senior official of another EU DPA conducted by the PI on 1 July 2014 ('Interview 3'), interview of a senior official of another EU DPA conducted by the PI on 8 July 2-14 ('Interview 4'), interview of a senior official of another EU DPA conducted by the PI on 11 July 2014 ('Interview 5), interview of a senior official of another EU DPA conducted by the PI on 6 June 2014 ('Interview 9), interview of a senior official of another EU DPA conducted by the PI on 5 December 2014 ('Interview 14'), and interview of the head of department of the team of a DPA that conducts Cloud Investigations by the PI on 4 December 2014 ('Interview 15').

[42] Interview of a senior legal counsel of one large multinational Cloud Provider conducted by the PI on 10 July 2014 ('Interview 10'), interview of a senior legal counsel of another large multinational Cloud Provider conducted by the PI on 8 July 2014 ('Interview 11'), interview of a senior legal counsel of another popular multinational Cloud Provider conducted by the PI on 16 September 2014 ('Interview 12'), and interview of another large multinational Cloud Provider conducted by the PI on 4 November 2014 ('Interview 13').

[43] Interview of a senior representative of one of the European institutions conducted by the PI on 11 July 2014 ('Interview 7') and interview of a senior representation of another European institution conducted by the PI on 26 June 2014 ('Interview 8').

[44] A valid sample size for qualitative interviews is one which does not prevent data saturation (e.g. recurrence of similar findings), theoretical saturation (e.g. multiple data sources supporting one conclusion) or informational redundancy. See Bryman (n 37, 425).

[45] Interviews 1, 2, 3, 4,5, 14 and 15 as well as examination of over thirty pages of relevant Google Search Engine results returned when phrases such as 'Investigations EU Data Protection Authorities' were queried as at 10 June 2014 and updated on 10 February 2015.

'corrected version' by using many methods including minimal tidying up to contextualise unclear comments.[46]

Interviews covered key themes, such as the practices, methods, and aims of Cloud Investigations, the actors participating in Cloud Investigations (and their relationships), the reasons why Cloud Investigations are used, and the factors which impact on Cloud Investigations (e.g. their outcomes[47]). In line with qualitative methods, the interviewer adopted flexible and non-leading interviewing techniques[48] (e.g. flexible interview guide) to ensure that the respondents could tell their own stories of Cloud Investigations. Multiple strategies were used to manage difficult interviews. For example, when the Principal Investigator asked commercially or legally sensitive questions (e.g. questioning the links between the Snowden revelations[49] and Cloud Investigations), such questions were carefully phrased to ensure that the respondents did not clam up.

We analysed our interview data by looking for patterns, similarities, and distinction within and across the interviews that shed light on the research questions.[50] This ensured rigorous[51] data analysis. We read the dataset in its entirety first without assigning any themes to it.[52] We then read the dataset over and over again, highlighted and annotated the relevant sections (e.g. explanation building and pattern-matching).[53] We used the highlighted extracts

---

[46] n 39, 148.

[47] Outcome means whether the investigation succeeds in bringing the operations and policies of the Cloud Provider in line with the relevant data protection laws.

[48] n 39, 51.

[49] Edward Snowden is a former contractor of the US National Surveillance Agency ('NSA'). In June 2013, Mr Snowden leaked the details of extensive internet and phone surveillance by the NSA. These leaks were followed by further revelations in several newspapers that the NSA directly tapped into the servers of various internet companies including multinational Cloud Providers such as Facebook, Google, Microsoft and Yahoo to track online communications. For more see 'Edward Snowden: Leaks that exposed US spy programme,' (BBC News 17 January 2014) < http://www.bbc.co.uk/news/world-us-canada-23123964> accessed 10 February 2015.

[50] This is a key aspect of rigour. See Bryman (n 37).

[51] For more on these data analysis techniques, see Robert K Yin, *Qualitative Research: Design and Methods* (Sage 2013).

[52] A key aspect of reliable qualitative research. See Bryman (n 37) and ibid.

[53] n 34, 155.

and annotations to generate self-explanatory descriptive themes which were close to the data.[54]

Moreover, we evaluated the discursive arrangements between the themes and the constituting sub-themes of each theme. We also reviewed the descriptive themes and sub-themes in order to group the themes which shared common meanings. Here we went back and forth to the data and also used theoretical notions (e.g. the concept of regulatory style[55]) to generate more abstract themes such as 'Multiple Regulatory Styles.' [56] Finally, we employed various strategies to ensure that our data analysis was valid. For example, we looked for the 'black swans' or empirical data which challenged our theoretical and empirical assumptions. [57]

Four arguments emerge from our data analysis. Firstly, Cloud Investigations are complex regulatory processes that often involve different co-operative relationships between various actors, such as DPAs operating under distinct data protection laws. In practice, manifold interactions and practices, such as facilitative instruments, are deployed to form and perform such collaborations which are key to ensure the consistent application and enforcement of common data protection principles in an increasingly globalised context. Complexity can also manifest itself through other factors, such as budgetary constraints and pressures from stakeholders including the press, which impact on key aspects of Cloud Investigations. How such complexities are resolved during Cloud Investigations can often involve intricate and context-specific strategies, such as delegating action to a third-party. Secondly, regulation through Cloud Investigation is dynamic as it involves constant activities from multiple actors, continually evolving regulatory styles and compliance attitudes. Consequently, the regulatory encounters between Cloud Providers and EU DPAs during an investigation can involve ceaseless change. Thirdly, Cloud Investigations can, at times, be contested as EU DPAs and Cloud Providers attempt to resist each other`s attempts to direct the investigation in particular ways. Finally, we argue that three reasons including the

[54] E.g. 'Attitudes of Cloud Providers to Cloud Investigations.

[55] E.g. see section 3.3 below.

[56] See section 3.4 below.

[57] GE Guba and YS Lincoln, 'Competing paradigms in qualitative research,' (1994) 2 Handbook of Qualitative Research 163.

benefits of rapport-building, and relocation of some of the operations of multinational Cloud Providers to Europe, can account for why Cloud Investigations are growing in frequency in Europe. Here we also underline how the construction of specific realities during some Cloud Investigations (e.g. compliance attitudes) can hamper the effectiveness of Cloud Investigations as regulatory tools in the sense of enforcing all the relevant data protection laws.

1.4 Structure

This deliverable is divided into four sections (excluding this section). In section two, we examine how the successful outcomes (in the sense of bringing the operations and policies of the Cloud Providers in line with the relevant data protection laws) of some Cloud Investigations can often depend in part on various types of collaborative relationships between DPAs, such as information exchange, and decision-making. In section three, we analyse four key factors which impact on various aspects of Cloud Investigations, namely, internal and external pressures faced by EU DPAs, regulatory enforcement styles, and compliance attitudes. In the final section, we account for the growth of Cloud Investigations in Europe and deal with the potential issue of 'constructed reality' during Cloud Investigations. Constructed reality refers to the idea that reality does not exist out there but rather is formed and performed in specific ways through particular interactions.[58] During Cloud Investigations, various types of information are arranged in particular ways to convey specific accounts, such as the account that the EU DPA has evaluated the Cloud Provider`s compliance with the relevant data protection laws.[59] Here we examine the potential impact of constructing specific accounts of verification (i.e. examining compliance) and redress (i.e. recommendations to bring the Cloud Provider`s operations and policies in line with the relevant data protection laws) on the regulatory process.[60]

---

[58] E.g. For more on the performance of truths including reality see Bruno Latour, *Reassembling the Social. An Introduction to Actor-Network-Theory* (Oxford University Press 2005).

[59] For more on the idea of constructing reality during other types of investigations, such as audits, see Marilyn Strathern, 'Abstraction and decontextualisation: an anthropological comment or: e for ethnography' (Undated Pre-Publication Draft) < http://virtualsociety.sbs.ox.ac.uk/GRpapers/strathern.htm> accessed 10 February 2015.

[60] Dziminski B et al, 'D:C-2.1 Report detailing conceptual framework,' (A4 Cloud, D 32.1, 13 October 2014).

2 Deploying Cloud Investigations as Regulatory Tools

Trans-jurisdictional co-operation by DPAs either through softer (e.g. information exchange) or more formal forms of collaborations (e.g. joint investigations of data controllers) has long been identified as a key component of the effective enforcement of data protection laws in an increasingly globalised context.[61] Effective enforcement means that shared data protection principles are applied and enforced consistently by EU DPAs.[62] If shared data protection principles are not applied and enforced consistently, this can erode the trust and respect of the citizens in such principles.[63]

The origins of trans-jurisdictional co-operation between EU DPAs can be traced to various legal frameworks, such as DPD, which imposes an obligation on EU DPAs to 'co-operate' with one another '…to the extent necessary for the performance of their duties, in particular by exchanging all useful information.'[64] Unsurprisingly, as with many other aspects of the DPD, the obligations of EU DPAs to co-operate with one another when exercising their regulatory functions are not fully fleshed out by the directive. Consequently, in practice, the enactment of the obligation of EU DPAs to co-operate with one another is subject to national implementing laws[65] and the EU DPAs` discretion.[66] Such national implementing laws can often be inconsistent in terms of fleshing out the EU DPAs` co-operative duties. For example, under the Irish Data Protection Act 1988 as amended in 2003, the Irish DPA has the power to authorise a person, including another EU DPA, in writing to exercise a number of powers

[61] E.g. Charles D Raab, 'Information privacy: networks of regulation at the subglobal level,' (2010) 1(3) Global Policy 291.

[62] C Reed, Making Laws for Cyberspace (OUP, 2012) 49ff; N Gunningham, 'Enforcement and compliance strategies,' in Robert Baldwin, Martin Cave, and Martin Lodge (eds) *The Oxford Handbook of Regulation* (OUP 2010) 120ff.

[63] See Reed (ibid).

[64] Also see Recital 64 of the DPD (n7). Also see Paragraphs 2 and 3 of the 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' <http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm> accessed 10 February 2015. The convention applies to all EU countries and beyond those all parties which have ratified this convention.

[65] E.g. For example, in France, Article 1 of the Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties as amended in 2004, 2009, 2010, and 2011 provides the following in relation to the French DPA`s duty to co-operate with other DPAs: 'The information technology must serve each citizen. Its development must be done within an international cooperation framework.'

[66] E.g. see n 59.

during investigations including the power to obtain information from the investigated data controller.[67] Other national implementing data protection laws in Europe do not make such provisions.[68]

Although the current literature in the fields of data protection and technology regulation has analysed how EU DPAs co-operate with one another generally, such analyses have approach this question from a doctrinal perspective. [69] There is sparse consideration of how EU DPAs collaborate with one another during investigations in practice.[70] This is particularly important given that vague provisions of the DPD on co-operation between EU DPAs and the inconsistent implementation of these provisions by European member states. In this section, we make a modest attempt to address this empirical gap by examining four various types of collaboration with DPAs during Cloud Investigations. In section 2.1, we examine three softer forms of collaborations between EU DPAs during Cloud Investigations, namely, information exchange, decision-making, and inclusion of plural data protection concerns. In section 2.2, we examine a more sustained and at times more formalised type of collaboration between some DPAs during Cloud Investigations, namely, the joint investigations of Cloud Providers.[71]

[67] Section 24, Data Protection Act 1988 as amended in 2003.

[68] For example, the Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés and the Decree of 20 October 2005 amended by the Decree of 25 March 2007 which regulate the investigative powers of the French DPA does not authorise the French DPA to appoint another party as an 'authorised officer' during its investigations.

[69] E.g. See Bygrave (n7).

[70] Ibid. But see Charles D Raab, 'Networks for regulation: privacy commissioners in a changing world,' (2011) 13(2) Journal of Comparative Policy Analysis 195.

[71] There are also other types of collaborations between DPAs, such as the privacy sweeps conducted by the twenty-six DPAs belonging to the Global Privacy Enforcement Network ('GPEN'), which can be relevant in the cloud context. However, we will not analyse these other collective initiatives as they have not triggered an investigation yet. This is hardly surprising given that the privacy sweep initiative has only been running for two years and mainly aims to '…gain the attention of the industry and privacy community' rather than investigate granularly if specific data controllers comply with the relevant data protection laws (Interview 15). For more on GPEN see < https://www.priv.gc.ca/media/nr-c/2014/bg_140910_e.asp> accessed 10 February 2015.

2.1 Pan-European Investigations: Trans-jurisdictional Co-operation in Context

Four out of our six EU DPA respondents have identified the meetings of the Technological Sub-Group ('TSG') of the Article 29 Working Party[72] ('A29WP') as an important space in which three soft forms of collaborations take place between EU DPAs during Cloud Investigations, namely, information exchange, decision-making, and inclusion of plural data protection concerns.[73] The Article 29 Working Party ('A29WP') is an advisory body which is composed of the representatives of the EU DPAs, the European Data Protection Supervisor[74] and the European Commission.[75] Its main tasks include promoting the uniform application of the DPD in all European member states as well as Norway, Liechtenstein and Iceland.[76] The A29WP holds five plenary meetings annually.[77] During the plenary meetings, various sub-groups of the A29WP, such as the Technology Sub-Group ('TSG'), also meet to address specific data protection issues raised by the Internet and similar technologies.[78] The agendas of the TSG meetings are set up according to the requests of the plenary meetings as well as current and proposed tasks of the EU DPAs.[79] So have the meetings of the TSG always been key in co-ordinating investigative actions?

According to some of our respondents (EU DPAs and EU institutions), the TSG meetings have not always operated as a forum through which the EU DPAs have co-

[72] Interviews 1, 2, 4, 9. See also <https://secure.edps.europa.eu/EDPSWEB/edps/Cooperation/Art29> accessed 10 February 2015.

[73] Ibid. For more on the role of the A29 WP in the context of the DPD, see Bygrave (n 7); Raab (n 68).

[74] The EDPS is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. For more see < https://secure.edps.europa.eu/EDPSWEB/edps/EDPS> accessed 10 February 2015.

[75] For more see < http://ec.europa.eu/justice/data-protection/article-29/index_en.htm> accessed 10 February 2015.

[76] 'Transferring your personal data outside the EU,' (EU Commission, last updated as 25 May 2014) <http://ec.europa.eu/justice/data-protection/data-collection/data-transfer/index_en.htm> accessed 12 February 2015.

[77] <https://secure.edps.europa.eu/EDPSWEB/edps/Cooperation/Art29> accessed 10 February 2015.

[78] ibid; Interviews 1, 2, 9.

[79] Interview 9, Email sent by the Principal Investigator to the EU DPA who participated in Interview 2.

ordinated their actions in relation to Cloud Investigations or investigations in general.[80] Some of our respondents suggest that the meetings of the TSG have become an increasingly important space through which EU DPAs co-operate with one another during Cloud Investigations since the investigations of the Google Street View technology of Google Inc. by various EU DPAs.[81] Briefly, Google Street View is a technology rolled out by Google Inc. in various jurisdictions to capture panoramic street pictures using a specially equipped camera mounted on a car.[82] In May 2010, Google Inc. publicly admitted that some of its Google Street View cars had inadvertently collected private information exchanged over unencrypted wireless networks.[83] Many EU DPAs investigated Google Inc. `s Google Street View feature from a strictly national rather than broader European perspective.[84] Consequently, such EU DPAs took distinct enforcement actions against Google Inc. in connection to its Google Street View.[85] For example, the UK DPA did not impose a fine on Google Street View but rather served an enforcement notice on Google Inc.[86] However, following their investigations, other EU DPAs, such as the Hamburg Commissioner for Data Protection and Freedom of Information, fined Google Inc.[87] Some of the inconsistent enforcement actions could be explained by national differences.[88] However, other variable enforcement actions could not be so easily rationalised. For example, many commentators

[80] E.g. ibid, Interview 1.

[81] See n 83 and 86.

[82] Ibid.

[83] 'WiFi data collection: An update,' (Google 14 May 2010) <http://googleblog.blogspot.co.uk/2010/05/wifi-data-collection-update.html> accessed 10 February 2015.

[84] E.g. interview 3.

[85] Interview 3.

[86] Google Inc. Enforcement Notice (UK ICO, 21 June 2013) < https://ico.org.uk/media/action-weve-taken/enforcement-notices/2527/google-inc-enforcement-notice-11062013.pdf> accessed 2 February 2015.

[87] Interview 3. Also see 'Hamburg watchdog serves Google with €145,000 fine over Street View data collection,' (Outlaw.com, 23 April 2013) < http://www.out-law.com/en/articles/2013/april/hamburg-watchdog-serves-google-with-145000-fine-over-street-view-data-collection/> accessed 2 February 2015.

[88] Interview 3.

criticised the UK DPA for not fining Google Inc.[89] Consequently, some EU DPAs were severely criticised by the media.[90] One of our EU DPA respondents suggests that this was a defining moment for many other EU DPAs as they recognised the need to work in concert with one another when investigating high-profile companies which raise pan-European data protection issues.[91] One of our respondents summed up the lessons learnt by many EU DPAs after the Google Street View investigations as follows: "Maybe we need to conduct our investigation differently at least when we work on similar topics, because otherwise we look a bit like idiots because we are contradictory."'[92] Although Google Street View technology is not a cloud-based technology, this case is important as it explains how co-ordinated investigations, facilitated by the TSG meetings, have started gaining momentum in Europe. Next, we now examine three ways in which EU DPAs co-operate with one another through the TSG meetings in the context of Cloud Investigations.

Firstly, EU DPAs exchange information with one another about ongoing and past Cloud Investigations[93] during the TSG meetings. The types of information which are exchanged depends on the approaches and powers of the relevant EU DPAs.[94] At times, some EU DPAs can update other EU DPAs about the status of an ongoing Cloud Investigation especially when the other EU DPAs have a regulatory interest in such investigations.[95] At other times, when an EU DPA is investigating a Cloud Provider, another EU DPA – which has already investigated this company - can provide the EU DPA with relevant documents or information (e.g. the correspondence between the organisation and

[89] E.g. Interview 3.

[90] Interview 3. Also see for example, 'Google escapes fine from ICO over Street View data collection and retention failings,' (Outlaw.com, 21 June 2013) < http://www.out-law.com/articles/2013/june/google-escapes-fine-from-ico-over-street-view-data-collection-and-retention-failings/> accessed 2 February 2015; Thomas Brewster, 'Exposed: ICO's Tame Investigation Of Google Street View Data Slurping,' (TechWeekEurope, 18 July 2013) <http://www.techweekeurope.co.uk/workspace/ico-google-street-view-wi-fi-investigation-failures-122287#1yh5OwBpQM0TseI1.99> accessed 2 February 2015.

[91] Interview 3.

[92] Interview 8.

[93] Interview 8.

[94] n 96.

[95] E.g. Interview 1.

the EU DPA).[96] One particular EU DPA often provides other EU DPAs with a copy of the unpublished investigation report to assist the other EU DPAs in assessing whether the Cloud Provider in question is breaching their national data protection laws.[97] An EU DPA`s willingness to share unpublished Cloud Investigations reports, will depend on its legal capacity and how far it perceives itself as being 'accountable' to other EU DPAs when it investigates multinational Cloud Providers which are 'established' in its jurisdiction for their European activities.[98] The exchange of information between EU DPAs in the context of Cloud Investigations continues in between the TSG meetings and can take various forms (e.g. emails and phone calls between EU DPAs).[99]

Secondly, the TSG meetings can be used as a platform for decision-making in the context of Cloud Investigations. Occasionally, one EU DPA can inform the rest of the TSG that it is concerned about the activities of a specific Cloud Provider whose services or operations fall within the remit of the TSG.[100] Here, the EU DPA discusses this matter with the TSG to decide whether to deal with its data protection concerns at a national level or at a European level through an investigation mandated by the A29WP.[101] When an investigation is mandated by the A29 WP, an EU DPA is appointed as the lead investigator and is responsible for conducting the various stages of the investigation, such as circulating the questionnaire, and conducting the on-site inspection if appropriate.[102] The appointment of an EU DPA as a lead EU DPA depends on several factors including whether it has pre-existing contacts with the Cloud Provider, its resources (i.e. does it have enough staff to investigate the various practices of the Cloud Provider), and expertise.[103] The lead EU DPA then regularly updates the rest of the TSG on the progress of its investigation. Here, other EU

[96] E.g. Interviews 1 and 2.

[97] E.g. Interview 1, 2, 3, and 4.

[98] Interviews 1, 2, 3, 4, 5, and 14.

[99] Interview 8.

[100] Interview 9.

[101] Interview 9.

[102] Interview 9.

[103] Interview 9.

DPAs can raise concerns about the progress or scope of the Cloud Investigation.[104] For example, during one mandated A29WP Cloud Investigation, some EU DPAs questioned how the lead EU DPA scoped the Cloud Investigation in terms of its initial limited examination of the data protection issues raised by the Cloud Provider.[105] At the end of such A29WP investigations, a number of recommendations are made by the lead EU DPA on behalf of the A29 WP to the Cloud Provider. During the TSG meetings, the lead EU DPA and other EU DPAs discuss and agree the recommendations.[106] In cases where the Cloud Provider fails to implement the agreed recommendations, as the A29WP has no enforcement powers, it is up to each EU DPA to enforce the agreed recommendations at national level. The lead EU DPA fully co-operates with the other EU DPAs in terms of sharing documents, information etc to assist them in enforcing the recommendations.[107] One should not assume that all EU DPAs co-operate with one to the same extent during Cloud Investigations. Indeed, some EU DPAs that are perceived as European leaders in the field of digital technologies can often remain silent during the TSG meetings. [108]

Thirdly, the TSG meetings can often be crucial in cases where an EU DPA, which considers itself to be the competent regulator for the European activities of a particular multinational Cloud Provider ('Competent Regulator'), conducts a Cloud Investigation. For some Competent Regulators, the TSG meetings can operate as a platform where other EU

[104] Interview 9.

[105] Interview 9.

[106] Interview 9.

[107] Interview 9. Typically, the EU DPA examines the findings of the A29WP mandated Cloud Investigations by applying its national data protection laws. Thus, in some jurisdictions (e.g. France), specific procedural steps will be following such as issuing a 'mise en demeure' or formal notice to the Cloud Provider to trigger the investigative process. For example, see Decision No. 2013-025 on 10 June 2013 by the Chair of the Commission nationale de l'informatique et des libertés giving formal notice to the company GOOGLE INC < http://www.cnil.fr/fileadmin/documents/en/D2013-025_10_Jun_2013_GOOGLE_INC_EN.pdf> accessed 10 February 2015 which triggered the investigation of Google`s Inc. amended privacy policies (which apply to its various services and technologies including its cloud-based email solution, namely, Gmail) by the French DPA.

[108] Interview 9.

.

DPAs can raise their own national data protection issues about the investigated Cloud Provider.[109] The Competent Regulator may then investigate these additional concerns during its investigation of that Cloud Provider.[110] During the TSG meetings, some Competent Regulators can evaluate if other EU DPAs have an interest in their ongoing or future Cloud Investigations. The Competent Regulator, then, determines on a case-by-case basis how best to deal with such plural interests during its Cloud Investigations.[111] The Competent Regulator also often carries on talking to the other EU DPAs that have a national interest in its Cloud Investigations after the TSG meetings.[112] For example, some Competent Regulators have informed other EU DPAs of the progress of their negotiations on relevant matters with the investigated Cloud Providers. On a strict legal analysis, the Competent Regulator, only has the obligation to ensure that the investigated Cloud Provider complies with its national data protection laws.[113] However, in practice, Competent Regulators can often recognise that the data protection concerns of other EU DPAs also have to be addressed during their Cloud Investigations.[114] Consequently, during such Cloud Investigations, some Competent Regulators '…oversee them [the Cloud Providers] rigorously and in a way which takes into account the legitimate interests of other…regulators particularly in the EU.'[115] In such cases, the Competent Regulators become a '…a proxy everybody [other EU DPAs] has to go through…'[116] to ensure that their data protection concerns about the operations of that Cloud Provider are adequately dealt with during the investigation.

[109] Interview 1.

[110] Interviews 1, 2, 3, 4, 5, and 14.

[111] Ibid.

[112] For example, because the data subjects who reside in their jurisdiction has filed a complaint about the specific Cloud Provider. Interviews 1 and 3.

[113] Interview 1

[114] Interview 1

[115] Interview 1

[116] Interview 3.

According to our interview data analysis, the TSG and its successor, if and when the General Data Protection Regulation (GDPR')[117] is enacted, will continue to operate as an important platform through which EU DPAs co-ordinate actions during Cloud Investigations for two reasons.[118] Firstly, there is an institutional move at EU level towards increased co-operation through joint investigations by EU DPAs.[119] For example, the GDPR has explicit provisions on joint investigations.[120] Secondly, as more and more multinational Cloud Providers have a strong European presence, they will increasingly raise data protection issues which are pan-European rather than confined to a specific national border. [121] Having analysed three specific forms of co-operation between EU DPAs during Cloud Investigations, namely, information exchange, decision-making, and inclusion of plural data protection concerns, in the next section, we examine one final form of co-operation between DPAs operating under distinct data protection frameworks, namely, how Cloud Investigations can be jointly conducted by DPAs operating under distinct data protection frameworks.

2.2 Cross-Border Joint Enforcement Action: Of Regulatory Capacities, Facilitative Instruments and Strategic Deliberations

The expanding global digital economy[122] has been accompanied by exponential transborder data flows which have raised significant global data protection issues that challenge DPAs.[123] As noted in section 2.1, the successful application of data protection laws largely depend on the effective enforcement of such laws. Effective enforcement of data protection laws can often be problematic when a global regulatory response rather than a national regulatory one

[117] GDPR (n 31).

[118] E.g. Interview 9.

[119] Interview 7.

[120] E.g. Article 56 of the GDPR (n 31).

[121] Interview 7.

[122] For more on the impact of the Digital economy, see 'Internet Matters: The Net`s Sweeping Impact on Growth, Jobs, and Prosperity,' (McKinsey, 2011) < http://www.mckinsey.com/~/media/mckinsey/dotcom/homepage/2011%20june%20internet%20economy/mgi_internet_matters_full_report.ashx>.

[123] E.g. see Chris Kuner, Transborder Data Flows and Data Privacy Law (OUP 2013).

is required.[124] Consequently, there have been renewed calls for more vigorous and concerted enforcement actions, such as joint investigations, by DPAs to address the data protection issues raised by cross-border data flows.[125] In this section, we analyse how DPAs are starting to investigate Cloud Providers in conjunction with one another.[126]

So how do joint investigations of a Cloud Provider come about? We propose a few tentative answers to this question based on the joint investigation of a Cloud Provider ('CP 4') conducted by two DPAs operating under different data protection laws ('Investigation 4').[127] This is an instructive empirical example for this deliverable as it shows how such types of high-level collaborations are organised so as to achieve effective transnational regulation in the sense of the consistent[128] application and enforcement similar high-level data protection principles. Tempting as it may be, we should not reach conclusions about joint Cloud Investigations that extend beyond the confines of the analysed data given that our findings relate only to one joint Cloud Investigation.

The deployment and outcomes[129] of Investigation 4 depended on three factors. Before moving on to these three factors, it is important to note that the analysis expounded in section 3.4 can also be relevant to joint Cloud Investigations. In fact, one of the potential obstacles to the outcomes of joint Cloud Investigation can be the compliance attitudes of Cloud Providers. However, we did not have access to CP 4 during our data collection and do not wish to speculate on its responses to Investigation 4. Nonetheless, this is a key area

---

[124] It is beyond the scope of this paper to charter the rise of mutual assistance between DPAs throughout history. For more see Raab (n 61).

[125] E.g. ibid.

[126] This form of co-operation is distinct from the A29WP-mandated investigations as the latter means that one DPA is in charge of all aspect of the investigations. It is beyond the scope of this paper to analyse the various forms of collaborations between DPAs which have emerged over the years, such as the declarations adopted by DPAs during the annual international conference of data protection and privacy commissioners. E.g. see 'The Declaration of Civil Society Organizations on the Role of Data Protection and Privacy Commissioners,' (Montreal, 25 September 2007) where the participating DPAs agreed, inter alia, that they '…must increase their own collective efforts' and make a 'concerted, cross-national. Also see Raab (n 71).

[127] Interview 15.

[128] As far as possible, taking into account national differences.

[129] Outcome means whether the investigation succeeds in bringing the operations and policies of the Cloud Provider in line with the relevant data protection laws.

which requires future research as it can potentially highlight how such international collaborative tasks can be dynamic by, for example, requiring constantly evolving regulatory styles and strategies to address the compliance responses of Cloud Providers.

Firstly, both DPAs required regulatory capacities in the sense of actual and potential capacities to work in concert with one another during the Investigation 4.[130] The regulatory capacities of both DPAs depended on several factors including the extent to which they could co-operate with one another during joint investigations under national laws, whether they had the resources to conduct a joint investigation (e.g. time, staff, and expertise), and whether they could identify common problems which would be resolved during the investigation.[131] For example, one of our respondents told us that it would not have had the regulatory capacity to participate in Investigation 4 if its national data protections were not amended a few years ago.[132] In particular, the legislative amendments provided this DPA with a broader capacity to co-operate with other DPAs during investigations including the power to share information and work in concert with other DPAs.[133]

Secondly, although the DPAs had the requisite regulatory capacities, Investigation 4 would not have been succeeded in bringing the operations of the investigated Cloud Provider in line with the shared data protection principles of the two DPAs if the regulatory capacities of the two DPAs, as set out in law, were not further fleshed out in facilitative instruments, such as memoranda of understanding. Both DPAs entered into a memorandum of understanding ('MoU1') before Investigation 4 was triggered.[134] For avoidance of doubt, MoU1 did not only govern how Investigation 4 would be carried out but also set out the

---

[130] Regulatory capacity is a complex concept which relates to the actual and potential '…possession of resources…the ability and willingness to use them' to regulate for specific purposes. For more see, Julia Black, 'Enrolling actors in regulatory systems: Examples from UK financial services regulation,' (2003) Public Law 63.

[131] E.g. Interview 15.

[132] Interview 15.

[133] Interview 15.

[134] Interview 15. Other instruments which can govern collaborative work between DPAs include the APEC Cross-border Privacy Enforcement Arrangement in which various regulators such as the Canadian DPA and the United States Federal Trade Commission have entered into since 16 July 2010. For more see <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx> accessed 10 February 2015.

responsibilities of each DPA during various types of collaborative tasks including investigations. Our analysis of the terms of MoU1[135] showed that most of the agreed terms were similar in scope and wording to the terms of other memoranda of understanding agreed between other DPAs.[136] However MoU1 was different from these other memoranda of understanding as it also explicitly identified joint investigations as an area of collaboration which had 'priority.'[137] MoU1 facilitated the conduct of this Investigation 4 by detailing the parameters within which cross-border enforcement co-operation would take place between the two DPAs.[138] For example, MoU1 detailed the resources which could be exchanged between the two DPAs and how collaborative tasks would occur in practice.[139]

Thirdly, beyond regulatory capacities and facilitative instruments, a number of practices by the DPAs also enacted Investigation 4. Although such practices are neither set out in law nor in MoU1, these practices are evidently framed to some extent by these (and potentially other) factors.[140] In terms of practices, both DPAs had to navigate through a rich and complex tapestry of distinct professional and local cultures in order to achieve the aims of Investigation 4.[141] To some extent, the two DPAs managed to overcome some of potential issues raised by these differences through their shared world views, namely, that the data

[135] The relevant Memorandum of Understanding is a public document. However, we cannot identify it as it would disclose the identities of our respondents. Also Interview 15.

[136] E.g. On 26 June 2013, the Irish DPA and the United States Federal Trade Commission entered into a Memorandum of Understanding which sets out the terms under which each party agrees to mutually assist one another when dealing with data protection issues. MEMORANDUM OF UNDERSTANDING BETWEEN THE UNITED STATES FEDERAL TRADE COMMISSION AND THE OFFICE OF THE DATA PROTECTION COMMISSIONER OF IRELAND ON MUTUAL ASSISTANCE IN THE ENFORCEMENT OF LAWS PROTECTING PERSONAL INFORMATION IN THE PRIVATE SECTOR (26 June 2013) <http://www.dataprotection.ie/documents/MOU/MOU.pdf> accessed28 January 2015.

[137] n 135.

[138] Ibid.

[139] Ibid.

[140] These interactions take place within the context of applicable laws and MoU.

[141] Interview 15.

protection issues raised by CP 4 required a joint response, a common[142]set of data protection principles derived from the applicable data protection laws (e.g. security) and similar regulatory roles (e.g. investigations).[143] This shared understanding did not exist in a state of nature but rather emerged from the constant conversations of and deliberations by the two DPAs.[144] As discussed later, the DPAs developed specific strategies to manage the differences which could not be overcome, such as their distinct enforcement powers.

Deliberations and consultations between these two DPAs were also key in fleshing out the specific regulatory capacities of the two DPAs. Before initiating Investigation 4, both DPAs engaged in substantial and 'up front' strategic discussions about how best to allocate the investigative responsibilities between them.[145] Here each DPA had to understand what the other could bring to the table in terms of resources and sector-specific expertise.[146] Following extensive deliberations, the two DPAs agreed that one DPA would be solely responsible for technically testing various operations of CP 4 whilst the other DPA would be in charge of communicating with CP 4.[147] Moreover, although each DPA had its own tasks, the other DPA would often contribute to the performance of such tasks where relevant. For example, although one of the DPAs was in charge of communicating with CP 4, such

[142] By using the term common, we do not imply that the differences between the data protection laws of specific jurisdictions are negligible. However, such an analysis is beyond the scope of this paper. We use the term 'common' to refer to the idea that at an abstract level, various data protection laws share common principles such as purpose specification and security. However, there can often be considerable variation in how such principles are implemented. For more, see Christopher Kuner, 'An international legal framework for data protection: Issues and prospects,' (2009) 25(4) Computer Law & Security Review 307.

[143] For more on the importance of shared world views in the context of concerted regulation, see Martin Lodge, Kai Wegrich, and Gail McElroy, 'Dodgy kebabs everywhere? Variety of worldviews and regulatory change,' (2010) 88(1) Public Administration 247. Also see Raab (n 70) on the areas of commonalities between DPAs generally.

[144] Other factors include the incremental move in the field of data protection towards concerted enforcement actions by DPAs to deal consistently with the data protection issues raised by cross-border data flows. See Raab (n 61, 68). For more on the roles of deliberations and discussions in producing shared views amongst actors, see Robert Baldwin, Martin Cave, and Martin Lodge. *Understanding regulation: theory, strategy, and practice*. (Oxford University Press 2012) 51ff.

[145] Interview 15.

[146] Interview 15.

[147] Interview 15.

communications were joint enterprises in the sense of being vetted by the other DPA before being sent to CP 4 and being sent under joint cover.[148]

Other potential issues, such as those raised by the distinct enforcement powers of each DPA, were successfully dealt with by both DPAs by acknowledging these national differences before initiating Investigation 4, agreeing on the strategies to accommodate these differences and bearing these strategies in mind during Investigation 4.[149]For example, in order to deal with their distinct enforcement powers, the two DPAs devised the following strategy. They investigated specific aspects of CP4, such as the adequacy of the security measures implemented by CP 4 to generate passwords for its users, by referring to shared data protection principles (e.g. security). Moreover, both DPAs worked in concert with one another to analyse their investigative findings and determine to what extent CP 4`s processing operations were in compliance with the shared data protection principles.[150] At this point, the two DPAs circulated a preliminary report of their findings to CP 4 to provide the latter with the opportunity to respond to the findings or implement specific changes before the final report was issued.[151] However, when tackling the final report, each DPA reached its own conclusions by applying its national data protection laws. The conclusions reached by each DPA at the end of Investigation 4 were similar although each DPA adopted different legal rules and procedures to reach such conclusions.[152] We will explore the implications of this finding in D-4.4. So what are the advantages of joint Cloud Investigations for the Cloud Provider and DPAs?

Joint Cloud Investigations have three key advantages for the DPAs. Firstly, joint investigations can often be more efficient than an investigation deployed by only one DPA. As one of our respondents says:

> '…you can use the analogy of football where you don't want everyone on the team all running to the ball at the same place or following the ball around the field. There is

[148] Interview 15.

[149] Interview 15.

[150] ibid

[151] Interview 15.

[152] Interview 15 and n 109.

> efficiency to be realised in identifying and playing positions. It can change for different investigations...'[153]

Thus, during Investigation 4, the two DPAs expanded their investigative capacities by allocating responsibilities to one another on the basis of available resources and expertise pool. In particular, both DPAs played to their strengths. The DPA that had more extensive expertise in testing the data processing operations and policies of CP 4 was responsible for technical testing.[154] Likewise, the DPA that had existing connections with CP 4 was responsible for managing the communications and interactions between the DPAs and CP 4.[155] This enabled the DPAs to investigate CP 4 more extensively than they would have been able to do if they conducted the investigation on their own.

Secondly, joint Cloud Investigations can often be appropriate regulatory tools used to convey an international response to an international data protection problem.[156]In particular, Investigation 4 had a transnational impact as the operations of CP4 were brought in line with the data protection laws of two countries.[157] This would not have been achieved if the two DPAs did not join forces.

Thirdly, a concerted Cloud Investigation can often provide DPAs with more leverage when they negotiate with the investigated Cloud Provider.[158] CP 4 paid greater attention to the investigation as it was dealing with more than one DPA[159] and was very much aware that each DPA would impose two distinct set of sanctions at the end of Investigation 4 if they were not satisfied with the outcomes of the investigation. Consequently, the potential deployment of sanctions by two DPAs operating under distinct data protection laws provided the two DPAs with greater leverage when they negotiated specific aspects of compliance

---

[153] Interview 15.

[154] Interview 15.

[155] Interview 15.

[156] Ibid.

[157] Interview 15.

[158] Interview 15.

[159] This comparison is context-specific. Here our respondent was noting how other Cloud Providers which it had investigated on its own do not always give priority to the investigative process.

with the CP 4 during the investigation.[160] Such leverage may not always be present during other types of collaborative Cloud Investigations, such as the ones which are mandated by the A29WP, as in such cases the Cloud Provider is still dealing with one DPA (acting on behalf of the A29WP) which has no specific enforcement powers within the context of such investigations.[161]

From the perspective of the investigated Cloud Provider, joint Cloud Investigations can be beneficial in two respects. Firstly, joint Cloud Investigations can often mean more 'robust results' in data protection terms.[162] In other words, the investigated Cloud Provider can be confident that its operations and policies comply with the data protection laws of more than one jurisdiction at the end of the investigation. Secondly, concerted Cloud Investigations can also eliminate redundancies for the investigated Cloud Provider as it does not have to engage with multiple DPAs. In effect, the Cloud Provider can respond to one aggregated set of questions from multiple DPAs, rather than distinct sets of questions, inspections etc from various DPAs.[163] Such redundancies are still present in other types of collaborative investigations such as the A29WP-mandated Cloud Investigations as if the Cloud Provider refuses to implement the recommendations of the A29WP at the end of the investigation, then each EU DPA has to initiate an investigation under its national data protection laws to enforce these recommendations nationally. In effect, this starts the investigative process from scratch as the Cloud Providers then have to respond to distinct sets of questions from multiple EU DPAs.

Having analysed how Cloud Investigations can be complex regulatory processes which often involve collaborations between several actors, such as multiple DPAs, next, we analyse other areas of complexities which are embroiled with Cloud Investigations, namely, pressures faced by EU DPAs, regulatory styles, and compliance attitudes.

---

[160] Interview 15.

[161] The A29WP has no enforcement powers. In such joint investigations, the EU DPA can only enforce its recommendations after an investigation if it initiates the investigation under its national data protection laws. E.g. Interview 2.

[162] Interview 15.

[163] Interview 15.

3 Cloud Investigations: Of Pressures, Regulatory Styles, Compliance Attitudes

Our data analysis shows that four factors, namely, internal pressures faced by the EU DPAs, external pressures faced by EU DPAs, EU DPAs` regulatory styles, and compliance attitudes of Cloud Providers, may have an impact on three aspects of Cloud Investigations, namely, whether and how (e.g. methods, practices, and aims) they are conducted, and their outcomes. Outcome means whether the investigation succeeds in bringing the operations and policies of the Cloud Provider in line with the relevant data protection laws.

Before proceeding with our analysis, it may be useful to clarify our approach in this section. As analysed in the preliminary D-4.11, as a baseline all Cloud Investigations aim to ensure that the activities of the investigated Cloud Providers comply with the applicable legislative framework. Invariably, many Cloud Investigations can have other aims, such as education and establishing best practice, depending on the jurisdiction and investigation in question. In this section, we analyse the factors which impact on whether the baseline goal is achieved. An inquiry into the possible factors which impact on whether the other aims of Cloud Investigations are achieved, though interesting, is not within the remit of this paper.[164] Moreover, in sections 3.1 and 3.2 below we only examine how the internal and external pressures faced by EU DPAs impact on Cloud Investigations. We do not analyse how potential internal and external pressures faced by investigated Cloud Providers impact on Cloud Investigations because our Cloud Provider respondents were not prepared to discuss this with us. However, we are not suggesting that investigated Cloud Providers are not subject to several internal and external pressures which impact on Cloud Investigations.[165] Finally, although we do not consider how and to what extent the inconsistent implementation of the DPD by European member states impact on Cloud Investigations, we are not suggesting that this is not an important analysis. However, after careful consideration, we have decided not to undertake this analysis for two reasons.

[164] This requires further data collection and analysis which cannot be undertaken due to the tight timeframe of T:D-4.1.

[165] Indeed some of our Cloud Provider respondents also pointed out how in the run-up to and during the Cloud Investigation, certain resources of the organisation is redirected or restructured to ensure that the company can interact with the EU DPA as well as provide it with the relevant information. Interview 11.

Firstly, this deliverable does not aim to rehash well-known arguments in the field of data protection law about the impact of the inconsistent implementation of the DPD by European member states.[166] Such an analysis befits a more traditional black-letter law empirical approach rather than a socio-legal approach which seeks to understand how law operates in context.[167] Secondly, many of our respondents have observed that despite the inconsistent implementation of the DPD and bearing in mind the recent ruling of the Court of Justice of the European Union that related instruments, such as, the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC,[168] are full harmonisation instruments[169], '…deep down there are not huge differences between European member states…when you step back a bit, you are talking about nuances.'[170] We are not underplaying the differences (whether procedural or otherwise) between the EU DPAs` enforcement powers but are rather emphasising how such differences may be of less consequence during some Cloud Investigations (e.g. joint investigations or a 'one-stop shop' type Cloud Investigation) where EU DPAs operate from a common approach to the main principles of the DPD during the earlier parts of the investigations and bring in the national data protection laws at a later stage (e.g. when they draft the report of the findings of their investigations).[171] Here, national implementing laws are strategically deployed to legitimise the findings of the Cloud Investigation. We will explore what this finding indicates about the role of law in regulating 'personal data' in cloud computing in D-4.4.

---

[166] E.g. see Yves Poullet, 'EU data protection policy. The Directive 95/46/EC: Ten years after,' (2006) 22(3) Computer Law & Security Review 206; declaration of the Article 29 Working Party on Enforcement, 25 November 2004, WP 101 which makes the case for the need to overcome national differences and move towards 'synchronised national enforcement actions'.

[167] n 4.

[168] OJ L 105, 13.4.2006, 54.

[169] Case 293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources et al (2014) < http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN> accessed 10 February 2015.

[170] Interview 1

[171] E.g. Interview 1,

3.1 Internal Pressures faced by EU DPAs

Unsurprisingly, our data analysis highlights that like many other regulators, EU DPAs often face internal[172] pressures which impact on how they exercise their regulatory roles including their investigative roles. Internal pressures refer to the financial pressures faced by EU DPAs which restrict their staff numbers[173] and other forms of expenditure such as travel costs.[174] This perennial problem is well-known.[175] What is unknown so far is how the lack of resources can affect Cloud Investigations. Three out of the six EU DPA respondents specifically identified that their limited resources can often have an effect on whether Cloud Investigation is deployed, its foci and its methods.[176] These three EU DPAs - which we call, DPA A, B, and C – have on average between ten to twenty employees.[177]

DPA A argues that its lack of resources means that it only investigates a Cloud Provider where there is a significant 'statistical'[178] number of complaints against the Cloud Provider.[179] Amongst our EU DPA respondents, DPA A is far more constrained by its resources than other EU DPAs when it comes to deciding whether to deploy a Cloud

[172] For more on how enforcement by regulators can often be constrained by their limited resources, see R Baldwin, M Cave, and M Lodge, Understanding Regulation: Theory, Strategy, and Practice (OUP 2012) 227ff. For more on the importance of sufficient resources for effective enforcement of laws by DPAs, see Article 29 Data Protection Working Party, 2004a, Declaration of the Article 29 Working Party on Enforcement. Brussels: European Union, pp. 1–5; Nouwt Sjaak ,'The Role of Data Protection Authorities,' in Yves Poullet, Paul de Hert, and Cécile de Terwangne (eds) *Reinventing data protection?* (Springer 2009) 136ff.

[173] E.g. Interviews 1, 2, 3,

[174] E.g. Interview 4.

[175] First report on the implementation of the Data Protection Directive (95/46/EC) of 15 May 2003 COM (2003) 265 final; European Union Agency for Fundamental Rights, 'Data Protection in the European Union: the Role of National Data Protection Authorities' (2010), <http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf>, at 42, accessed 12 February 2015, finding that eleven out of twenty-seven national data protection authorities in the EU Member States were unable to carry out the entirety of their tasks because of a lack of financial and human resources

[176] Interviews 1, 3 and 4.

[177] Ibid.

[178] It is unclear whether there is a specific numerical threshold here which has to be reached before an investigation is triggered.

[179] Interview 3.

Investigation.[180] Specifically, its limited resources means that although at times DPA A wishes to investigate a Cloud Provider, it is '…simply unable to do [so] because we are so few people and are unable to, in a structured way, control and monitor the companies in our scope of regulation (sic).'[181] This also means that when DPA A investigates a Cloud Provider it is often unable to investigate in detail the operations of the Cloud Provider. Consequently, certain types of investigative practices, such as reviewing the privacy and security policies and reviewing (rather than testing) small algorithmic sequences, are privileged during the Cloud Investigation over other types of investigative practices (e.g. testing code, on-site visits) as they are not as draining on the resources of DPA A.[182] Evidently, DPA A`s initial fact-finding during Cloud Investigations it likely to be limited. Consequently, the outcomes of its Cloud investigations are also likely to be limited (e.g. the number and types of recommendations issued at the end of the investigation).[183] The deeper dive into the processing operations of the Cloud provider in terms of analysing every single processing operation, and technically testing crucial programming sequences (e.g. the programme designed for deleting specific cookies) often remains an 'ideal' rather than a reality for DPA A.[184]

In contrast to DPA A, DPA B deals with its restricted financial and human resources in another way. DPA B`s team is of a similar size to DPA A`s team.[185] However, DPA B has investigated several multinational Cloud Providers that are 'established' in its jurisdiction for their European activities. Although DPA B`s limited resources impact on how it generally exercises its investigative powers, when it comes to such Cloud Providers, DPA B deals with the financial pressures by balancing scarce resources with efficiency.[186] DPA B performs this balancing exercise when it plans its investigations for the forthcoming year as well as when it

[180] Interview 3

[181] Interview 3.

[182] Interview 3.

[183] Interview 3.

[184] Interview 3, 9

[185] Interviews 1 and 3.

[186] E.g. Interviews 1, 2, 3, 4 and 14.

decides to conduct an on-the-spot investigation.[187] The balancing exercise takes into account various factors including legal obligations, media interest in the operations of specific Cloud Providers, data protection concerns of other EU DPAs about specific Cloud Providers and complaints filed by data subjects against such companies.[188] As DPA B explains:

> '…We have limited resources. So … our focus is very much on being efficient and we are pretty ruthlessly efficient. But at the end of the day, that includes being able to demonstrate that we have done a good job….So yes we are efficient but we do not skimp on the work. When dealing with multinationals we are very thorough because we have that broader accountability to other regulators and the general public and so on.'[189]

This extract is significant as it emphasises how the pressures which DPA B faces from other stakeholders, such as other EU DPAs, play a key part in the balancing exercise. We will revisit the topic of external pressures in more detail in section 3.2.

For now it suffices to say that DPA B`s 'broader accountability obligations' or its concern with demonstrating to other stakeholders that '…[it] ha[s] done a good job' influence how it allocates its limited resources.[190] Consequently, the multinational Cloud Providers are often 'prioritised' in terms of allocating resources for investigations as DPA B often feels pressure from external sources to show that it has regulated such companies to '…European standards'.[191] DPA B 'does not skimp on the work' in such investigations and undertakes a

---

[187] Ibid.

[188] Ibid.

[189] Ibid.

[190] Ibid.

[191] Ibid. Targeted enforcement have been used by regulators in various fields as a strategy to overcome their limited enforcement. E.g. for use of targeted enforcement in environmental regulation see Peter May, and Soren Winter, 'Reconsidering Styles of Regulatory Enforcement: Patterns in Danish Agro-Environmental Inspection,' (2000) 22(2) Law & Policy 143; Sarah L Stafford, 'Self-policing in a targeted enforcement regime,' (2008) Southern Economic Journal 934. For use of targeted enforcement in financial regulation see Howell E Jackson, 'Variation in the intensity of financial regulation: Preliminary evidence and potential implications,' (2007) 24 Yale J. on Reg. 253. A review of the current literature on the regulation of personal data indicates that there has been no

detailed examination of all the relevant aspects of the Cloud Provider including technically testing all its operations where appropriate.[192] Additionally, in cases where the investigated Cloud Provider has extremely complex technical operations, DPA B often employs novel strategies to ensure that it can test every relevant data processing operations. For example, in one of its past Cloud Investigations, DPA B hired a technical expert from a local university to test every single processing operation including the data structures which were exchanged between the mobile application version of the site and mobile devices (e.g. mobile phone) on which the application was installed.[193] In its current Cloud Investigations, DPA B is considering various options to boost its technical testing capacities including using trusted sub-contractors and exploring whether the Cloud Provider is willing to shoulder the cost of hiring sub-contractors who operate under the instructions of DPA B for the purposes of the investigation.[194] Consequently DPA B overcomes its limited resources in the context of Cloud Investigations by delegating part of the investigative tasks to sub-contractors.[195] This is an important finding which challenges current understandings of the investigation by an EU DPA as a regulatory tool which operates in a linear direction from the EU DPA to the Cloud Provider. Even at EU DPA level, there can often be complexities in terms of which actors (other than the EU DPA) perform certain investigative tasks. We will explore the significance of this finding in D-4.4. Complexity does not only appear at EU DPA level but also at the level of Cloud Providers, as analysed in section 3.4. Finally, after such Cloud Investigations, DPA B often offsets the potential financial impact of these investigations by publishing guidelines which apply to companies which operate in the same industry as the investigated multinational.[196] EU DPAs that strategically determine[197] which Cloud Providers to fully[198]

---

substantive empirical analysis of targeted enforcement by DPAs. See Carey (n 6), Newman and (n 24), Bygrave (n 7) for examples of the examinations of the DPA`s enforcement practices.

[192] n 201.

[193] Ibid.

[194] Ibid.

[195] Ibid.

[196] Ibid.

[197] Where a complaint has been filed by a data subject, most EU DPAs have a duty to look into such complaints. However, this does not involve a duty to trigger a full blown investigations of the data controller (e.g. onsite inspection and request for information). This is a matter for the EU DPA`s discretion. Other reasons why EU DPAs can initiate an investigation of a data controller include

investigate (in the sense of on-site visits and testing their data processing operations), can often be better equipped at allocating their resources more effectively whilst at the same promoting the image of a proactive regulator.[199] In the words of one of our respondents, '…it is useful to pick off some of the big fish, as it were, to go back to the fishbowl analogy, but obviously it's not going to be possible to do [investigations] across a full spectrum of data controllers.'[200]

The last EU DPA in our trio of DPAs – DPA C – employs other strategies to cope with its limited resources.[201] DPA C`s exiguous finances means that the inspection part of its Cloud Investigations - can often be problematic as it can be costly for DPA C to travel to the premises of the investigated Cloud Provider.[202]In order to address this problem, DPA C has entered into a memorandum of understanding[203] ('MoU2') with a specialist financial agency of the state security[204] ('Financial Police') pursuant to which the Financial Police undertakes the inspection part of the investigation on behalf of DPA C.[205] In this jurisdiction, the Financial Police is primarily responsible for dealing with financial crime and smuggling. Before proceeding to this analysis, it is important to note that DPA C has not yet used the Financial

reports of data breaches in the press, publicly known data protection risks in specific industry sections. Interviews 1, 2, 3, 4.

[198] Most EU DPAs, such as the Italian DPA, have the obligations to investigate any complaint filed by the data subject. See sections 149 and 150 of the Legislative Decree No. 196/2003. However, most EU DPAs have the discretion to decide whether to initiate a full-blown investigation (e.g. onsite inspection, request for information) depending on the case in question. Similar provisions apply to other EU DPAs, such as the Hamburg DPA. See s 38, sub-s 1, sentence 7 in conjunction with s 21, sentence 1 of the Bundesdatenschutzgesetz ('BDSG') which imposes the duty on data protection authorities in Germany such as the Hamburg DPA to investigate a complaint filed by an individual against a data controller.

[199] E.g. Interview 12.

[200] Interview 12.

[201] Interview 4.

[202] Interview 4

[203] Interview 4. We have seen a copy of the relevant MoU which is partly a public document. We cannot refer to the MoU as this would disclose the identity of our respondent.

[204] This label is not entirely accurate but has been adopted to prevent the identification of the EU DPA.

[205] Interview 4.

Police to conduct its current Cloud Investigations.[206] However, it anticipates doing so in its upcoming Cloud Investigations.[207] Consequently, this analysis is important to shed light on other ways in which other EU DPAs can delegate action to other actors during Cloud Investigations.

DPA C has the power to require the assistance of other state agencies when it inspects the premises of data controllers during its investigation.[208] As part of MoU2, the Financial Police has created a special unit which assists the DPA C in inspecting specific data controllers. MoU2 is key here as it governs the relationships between DPA C and the specialised data protection unit of the Financial Police. For example, MoU2 specifies the legal and procedural parameters within which the special unit must act, and the duty of the special unit to act on the instructions of DPA C when it inspects the premises of data controllers.[209] The specialised unit is trained by DPA C. For example, DPA C makes the specialised unit fully aware of its legal obligations, its investigative powers, the procedural rules governing the conduct on an on-site inspection, the legal obligations and rights of data controllers, and the types of evidence which DPA C requires in order to assess whether the investigated company complies with data protection laws.[210] DPA C argues that by delegating part of the investigative exercise to such specialised units it can not only reduce its costs but also obtain '…good results, in particular … given the specialised unit become more specialised because they become more familiar with the issues and know what to look for… (sic).'[211] Delegating action can lead to complications, such as integrating the inspection results with the remaining tasks performed by DPA C during the Cloud Investigation (e.g. policy review, code testing etc).[212] Further complications may arise when the multiple 'selves' of the Financial Police come into conflict with one another. For example, occasionally, the

[206] Interview 4.

[207] Interview 4.

[208] E.g. Interview 4.

[209] E.g. Interview 4

[210] Ibid.

[211] Ibid.

[212] Ibid.

Financial Police can detect data protection issues when they undertake their own investigations of financial crime and smuggling cases. Here, these multiple selves need to be managed by, for example, reporting the detected data breaches to DPA C which may then investigate them if appropriate.[213] If internal pressures can generate specific complexities during Cloud Investigations, external pressures can also generate other intricacies during Cloud Investigations, as analysed next.

3.2 External Pressures Faced by EU DPAs

Most of our EU DPA respondents are pressured by other stakeholders, such as the press, when they investigate a Cloud Provider.[214] However, only one of our EU DPA respondent has been willing to explore this at length with us.[215] This might be explained by the fact that this EU DPA often investigates Cloud Providers which operate across Europe rather than merely in one jurisdiction. Important lessons can be drawn for this EU DPA`s experience especially for other EU DPAs that may act as 'one-stop' regulator if and when the GDPR comes into force.[216]

During its high-profile Cloud Investigations this EU DPA faces significant pressure from the media, NGOs and advocacy groups.[217] When it comes to the press, the Commissioner of this EU DPA ('Commissioner') receives daily calls from the international media asking him to comment on the progress of an ongoing investigation or asking him whether he will investigate a specific Cloud Provider that has suffered a serious data breach.[218] This Commissioner is also pressurised by the media coverage of its Cloud Investigations which can often be couched in negative terms.[219] Such abrasive media coverage can often lead to further complaints about the Cloud Provider from advocacy

[213] Ibid.

[214] E.g. Interviews 3, 4, and 5.

[215] E.g. Interviews 1, 2, 3, 4, 5, and 14.

[216] Ibid.

[217] Ibid.

[218] Ibid.

[219] Ibid.

groups.[220] This Commissioner also faces substantial pressure from other stakeholders, such as NGOs and advocacy groups, during and at the conclusion of its Cloud Investigations.[221] In his words, '…we [my team and I] are '…very conscious of being in a glass bowl' as many large companies relocate to his jurisdiction for the purposes of their European activities.[222] Consequently, the Commissioner and his team are often constantly under 'critical scrutiny' by various stakeholders who want to be assured that such Cloud Providers are not breaching European data protection laws.[223] Some of these stakeholders, such as the advocacy groups, can be 'fairly hostile'[224] in terms of putting their points across to the Commissioner during its Cloud Investigations. Despite this, the Commissioner is 'very open' when dealing with such stakeholders and answers their questions as best as he can subject to his duty of confidentiality.[225] As he says, '…we don't hide'[226] from those external stakeholders who seek accounts of how such Cloud Providers are being regulated. Consequently, by frequently engaging with such stakeholders and publicising the findings of his investigations either by publishing the full investigative report or summarising the main findings of the Cloud Investigation through press releases, to some extent this Commissioner can navigate around such external pressures.[227]

3.3 Regulatory Enforcement Styles of EU DPAs

Apart from internal and external pressures, another factor which impacts on Cloud Investigations is the regulatory enforcement styles of the EU DPAs.[228] Through our analysis

---

[220] Ibid.

[221] Ibid.

[222] Ibid.

[223] Ibid.

[224] Ibid.

[225] Ibid.

[226] Ibid.

[227] Ibid.

[228] For an introduction to different regulatory styles, see R Baldwin, Better Regulation: The Search and the Struggle in *Robert Baldwin, Martin Cave, and Martin Lodge (eds) The Oxford Handbook of Regulation (OUP 2010).*

of regulatory styles in this section and compliance attitudes in section 3.4, we underline how regulation through Cloud Investigations can be dynamic as it involves constantly evolving actions and interactions. We also analyse that regulation through Cloud Investigations can also be contested at times through an analysis of some of the resistance practices of Cloud Providers. Regulatory enforcement styles vary from EU DPA to EU DPA depending on factors, such as the applicable administrative laws,[229] the EU DPAs` enforcement powers,[230] and the responses of the investigated Cloud Providers (as analysed in section 3.4).

Our empirical data suggests that EU DPAs can adopt different regulatory styles during one Cloud Investigation depending on how the Cloud Provider responds to its regulatory strategies. Recent theoretical and empirical approaches to regulation conceive of regulatory styles in terms of regulatory strategies which escalate from soft strategies (e.g. advice) to more coercive strategies (e.g. fines) as the regulatee persists in defying the law[231] rather than belonging firmly to the 'punish'[232] or 'persuade'[233] camp. One key finding from our data analysis which is not covered by the relevant literature is that during Cloud Investigations, regulatory styles are not deployed in a linear direction (i.e. from soft to hard regulatory strategies) but rather dynamically (e.g. from soft to hard to soft again etc) depending on whether the Cloud Provider is unresponsive, recalcitrant, or incompetent or otherwise and the stage[234] of the Cloud Investigation. The Cloud Provider is not seen as a

---

[229] For example in France, where a data controller fails to implement the recommendations of the French DPA, the matter is then referred to the Sanctions Committee of the French DPA which determines the sanction which will be imposed on the data controller. See Article 45 (n 68).

[230] E.g. Some EU DPAs, such as the French DPA, have the power to fine data controllers whereas other EU DPAs, such as the Irish DPA, do not have such powers. See n 68 and n 21 for the relevant French and Irish data protection laws.

[231] In the limited sense of formal rules which are laid down in statutory instruments, and judicial decisions. See I Ayeres and J Braithwaite, *Responsive Regulation: Transcending the Deregulation* Debate (Oxford University Press 1992).

[232] See Gunningam (n 62).

[233] See B Hutter, Regulating Employers and Employees: Health and Safety in the WorkPlace,' (1993) 20(4) Journal of Law and Society 452.

[234] As examined fully in the preliminary D-4.11, Cloud Investigations have three stages, namely, the pre-investigative, investigative and post-investigative stages. The pre-investigative stage includes a plethora of circumstances, practices, and routines which lead to the investigative stage, such as email exchanges and conference calls between the EU DPA and Cloud Provider. The investigative stage starts when the EU DPA initiates the Cloud Investigation (e.g. by sending a 'letter of intention to audit'

static actor that behaves in only one way during the regulatory encounter. Consequently, regulatory encounters between the EU DPAs and Cloud providers are fluid rather than static ones.[235] Although, we analyse the compliance profiles of Cloud Providers (e.g. unresponsive etc) in section 3.4, we may refer to them in this section where relevant to our understanding of the regulatory styles of EU DPAs during Cloud Investigations.[236]

During the pre-investigative stage[237], most EU DPAs engage in substantial and lengthy discussions with the investigated Cloud providers over a long period of time (e.g. one year plus) to persuade the Cloud providers to meet the obligations under data protection laws.[238] Persuasive arguments can take various forms as explained next. Typically, at the outset, many EU DPAs interact with the Cloud Providers on the assumption that they are well-intentioned but perhaps ill-informed companies that are unaware of their data protection obligations.[239]As one of our respondents says:

> '…we do not go in on the assumption that you are breaking the law. We are going in on the basis that you are dealing with a complex area of law and if you are an American entity you have to domesticate to EU standards. And we are here to help you.'[240]

Here, EU DPAs educate the Cloud Providers about their data protection rights and obligations and explain to them which particular processing operation or policy provision breach the applicable laws.[241]

---

to the Cloud Provider) and ends when the investigation report is finalised and/or published (depending on whether the report is published). The post-investigative stage refers to the stage following the publication (whether internal or external) of the investigation report.

[235] For more on the links between regulatory strategies, regulatory styles, and encounters see Valerie Braithwaite et al, 'Regulatory Styles, Motivational Postures and Nursing Home Compliance,' (1994) 16(4) Law & Policy 363.

[236] This is a well-established theoretical and empirical point in the wider regulatory field. E.g. see Ayres and Braithwaite (n 231).

[237] See n 239.

[238] E.g. Interviews 1, 2, 3, and 4.

[239] n 144, 230ff.

[240] Interview 1.

[241] E.g. Interview 1.

However, EU DPAs can deploy other regulatory styles and strategies during subsequent stages of the Cloud Investigations if the Cloud Providers become recalcitrant. For example, one of our EU DPA respondents investigated a well-known multinational Cloud Provider which offers a suite of cloud solutions to corporate users.[242] The central question raised by this investigation was whether the personal data[243] processed by the data controller[244] (i.e. the Cloud Provider) would be transferred to a third-party country.[245] Initially, the Cloud Provider was reticent to provide the EU DPA with any information about whether personal data were transferred to a third-party country during processing.[246] At first, the EU DPA assumed that the company was not aware of the relevant data protection laws. Consequently, on several occasions, the EU DPA explained to the Cloud Provider the restrictions which were imposed on third-party transfers by its data protection laws. At that point, the Cloud Provider countered that it could not precisely know where the personal data in question were at any given moment in time '…due to the nature of cloud computing [which means] that data [were] constantly circulating around.' The EU DPA realised that it was not dealing with an ill-informed regulatee but rather a well-informed regulatee which was employing a series of distinct arguments to evade compliance.[247]

The EU DPA persevered in questioning the Cloud Provider about its knowledge of the location of the data at all times during processing as it was increasingly apparent to this EU DPA that the company in fact knew where the data would be stored. After a while, this EU DPA changed strategy and used economic arguments to persuade the Cloud Provider to give to the EU DPA specific assurances regarding data transfers.[248] Thus, during one encounter, the EU DPA informed the Cloud Provider that it would be unable to market its

[242] Interview 14.

[243] Ibid.

[244] Ibid.

[245] Interview 14.

[246] Ibid.

[247] Interview 14.

[248] Interview 14.

suite of cloud solutions in its jurisdiction unless it could guarantee where data would be transferred during processing.[249] Here, the wayward Cloud Provider agreed to provide the EU DPA with a guarantee that the personal data would not be transferred to any other country outside of the EEA except the United States of America where the company and its subsidiaries were safe harbour certified.[250]

Another example derived from our data analysis highlights how EU DPAs can escalate and de-escalate their regulatory styles and strategies within the same Cloud Investigation. Here, this EU DPA was investigating a multinational Cloud Provider that had a physical presence in its jurisdiction for its European activities. Consequently, this EU DPA was the DPA which had jurisdiction over this Cloud Provider`s European operations.[251] At the start of this investigation, this EU DPA used numerous soft tools, such as informing the Cloud Provider about its data protection obligations, and learning about its business operations, through numerous and regular interactions with the senior employees of the relevant teams of the Cloud Provider including management, public policy, and engineering.[252] Subsequently, the EU DPA thoroughly inspected most of the data processing operations and policies of the Cloud Provider to evaluate whether they complied with the applicable legislative framework.[253] The EU DPA made an informal preliminary assessment of compliance which it explained to the Cloud Provider.[254] Both parties engaged in lengthy negotiations to reach mutually acceptable solutions (i.e. solutions which would bring the Cloud Provider`s operations and policies in line with the relevant laws whilst not damaging its business interests).[255] However, at one point during the Cloud Investigation, the otherwise

[249] Ibid.

[250] Ibid.

[251] We should clarify that this does not necessarily preclude other EU DPAs from investigating this Cloud Providers. At the times of this Cloud Investigation, another EU DPA was also investigating this Cloud Provider with limited success as the Cloud Provider refused to engage with the EU DPA on the grounds on lack of jurisdiction. E.g. Interview 1.

[252] Interviews 1 and 13.

[253] Ibid.

[254] Ibid.

[255] Ibid.

co-operative Cloud Provider, started objecting to some of the recommendations of the EU DPA.[256] In particular, the Cloud Provider was unwilling to implement some recommendations which were designed to bring its operations and policies in line with the data protection laws of another European member state.[257] Here:

> '….in [this investigation] at the last moment it could have turned out a different outcome. There could have been a bit of an enforcement action been taken by us. There was a bit of a breakdown in communication…(sic)'[258]

At that point, the interactions between the Cloud Provider and the EU DPA became very strained.[259] The EU DPA threatened the Cloud Provider that it would initiate a stronger enforcement action against it.[260] The Cloud Provider retaliated that the EU DPA did not have the power to impose recommendations which were derived from the national data protection laws of another European jurisdiction.[261] Unfazed, the EU DPA retaliated in kind '…you say I can't do this…I say…ok take me to court.'[262] All in all, in the words of this EU DPA, at this stage, the approach was '…very unlegal.'[263] Eventually the EU DPA managed to persuade the Cloud Provider to change its stance by using its wider connections in another branch of the Cloud Provider.[264] Once the Cloud Provider agreed to implement all the recommendations of the EU DPA, the latter de-escalated its regulatory style to a more co-operative one. As this EU DPA says:

> "…Once the company is co-operating we stand behind the company. We will say they did co-operate. They are committed to doing it. We are satisfied in so far that we can

---

[256] Ibid.

[257] Ibid.

[258] Interview 1.

[259] Interviews 1 and 13.

[260] E.g. interview 1.

[261] Interviews and 13.

[262] E.g. interview 1.

[263] Ibid.

[264] N 3.

> be that they will be compliant once they implement these recommendations. I have used this phrase before: 'we beat people up behind closed doors and then come out smiling.'"[265]

The escalation and de-escalation of regulatory styles and strategies are not always apparent to another stakeholder (e.g. general public) as the 'messiness' and fractious aspects of the Cloud Investigations can often be glossed over in cases where the findings of the Cloud Investigations are published. We deal with the impact of such constructed realities on Cloud Investigations in section 4.2.

Additionally, in some cases, de-escalation may not always be possible once matters have been escalated. Where the Cloud Provider does not respond to specific threats of the EU DPA following a Cloud Investigation, such as the threat to fine the Cloud Provider, then some EU DPAs have no other option than to impose such fines.[266] It is clear that for most EU DPA this level of escalation is seen as the 'last resort'[267] when they are dealing with large multinational Cloud Providers that are unwilling to bring their activities in line with the relevant laws. One can question the effectiveness of fines as in cases where EU DPAs have imposed them after Cloud Investigation, such fines have not brought about a systematic change in terms of its data protection operations and policies. [268] This finding is limited to one specific Cloud Provider that refused to implement the recommendations of several EU DPAs following their Cloud Investigations.[269] Its non-compliance attitudes can be partly explain by its deep pockets and its treatment of such fines as '…the cost of doing business'[270] in Europe.

So which regulatory style secures the best outcome, in terms of bringing the current operations of the investigated Cloud Provider in line with data protection laws? Our data analysis suggests that regulatory styles which can seamlessly move from one end of the

[265] Interview 1

[266] E.g. Interview 2.

[267] E.g. Interviews 2, 3, and 14.

[268] E.g. Interview 1.

[269] E.g. Interviews 1, 2, 3, 4, 5.

[270] Interview 1

spectrum (soft) to the other (hard) and back are the most effective ones. Moreover, regulatory styles which recognise the 'business drivers' of the Cloud Providers[271], make attempts to find mutually convenient solutions, and do not rely heavily on formalistic tools have so far yielded better outcomes.[272]Regulatory styles and strategies do not exist in a vacuum and as mentioned earlier there is a close interaction between regulatory styles and the attitudes of Cloud Providers towards compliance. Next, we examine the motivations and behaviours of Cloud Providers during Cloud Investigations and their repercussions on the outcomes of Cloud Investigations.[273]

3.4 Cloud Providers: Of Plural Motivations

The DPD[274] makes specific provisions about the investigative powers of EU DPAs (e.g. power to collection information etc) which concurrently impose implicit (in the sense of unspecified) obligations on the investigated data controllers, such as, the obligation providing access to the requested information. Evidently, the obligations of data controllers to provide the EU DPA with access to the requested information and/or premises have been inconsistently fleshed out by the implementing national data protection laws. Thus, even if the national laws implementing the DPD impose a duty on data controllers to co-operate with EU DPAs during their investigations, such laws invariably do not specify the extent to which the data controllers have to be open and transparent with the EU DPAs during the investigations or may provide the data controllers with a right to withhold information in specific circumstances. So to what extent are Cloud Providers open and transparent with EU DPAs during investigations? Our data analysis shows that Cloud Providers can often be motivated to be open and transparent (to varying degrees and subject to commercial considerations) during Cloud Investigations for three reasons.

---

[271] Interview 1

[272] E.g. Interview 14, 3, 2

[273] It is commonly accepted in the field of regulation that empirical attention should be paid to the motivations and behaviours of the regulated to enable us to understand the relationships between the regulator and regulated. E.g. see Christine Jolls, Cass R Sunstein, and Richard Thaler, 'A behavioral approach to law and economics,' (1998) Stanford Law Review 1471.

[274] Article 28(3), DPD (n 7).

Firstly, some Cloud Providers are often motivated to be open and transparent (subject to the above caveat) with the EU DPAs during Cloud Investigations to generate trust with their customers. [275] Trust[276] refers to the reliance of the customers on the competence and willingness of Cloud Providers to look after rather than harm the data that have been entrusted to their care.[277] Many Cloud Providers interact openly and transparently with EU DPAs during Cloud Investigations to generate various dimensions of trust, such as commitment (demonstrating to their customers that they are committed to protecting their data), competence (showing to their customers that they operate in accordance with existing laws), and predictability (showing to their customers that the Cloud Providers will continue interacting with the EU DPA after the Cloud Investigation to ensure that its future processing operations or technologies or policies are in accordance with the relevant laws).[278] Cloud Investigations can often be effective and persuasive tools used by Cloud Providers to inform their customers that they '… can trust us with their data…trust that we are doing the right choices when it comes to processing their data.'[279] A positive Cloud Investigation – that is one which concludes that the Cloud Provider is mostly compliant and will rectify areas of non-compliance within a specific timeframe under the supervision of the EU DPA – can often reassure the customers of the Cloud Provider because a 'trustworthy…third party…acting for the state'[280] has assessed its compliance with existing laws as well as will carry on monitor its future compliance.

---

[275] In the field of regulation, there is a wide empirical literature on the plural motivations of the regulated to comply or not. E.g. See Harold G Grasmick, and Robert J Bursik Jr, 'Conscience, significant others, and rational choice: Extending the deterrence model,' (1990) Law and society review 827.

[276] It is beyond the scope of this paper to undertake a comprehensive analysis of the multidisciplinary literature on the concept of trust. For more on trust, see Wouter Poortinga and Nick F Pidgeon, 'Exploring the dimensionality of trust in risk regulation,' (2003) 23(5) Risk analysis 961. For more on trust, and cloud computing, see D:C-6.1: Risk and trust models for accountability in the cloud (D 36.1, A4 Cloud, 2 January 2014).

[277] A C Baier, 'Trust and antitrust,' (1986) Ethics 236.

[278] See R EKasperson, D Golding & S Tuler, (1992). 'Social distrust as a factor in siting hazardous facilities and communicating risk,' (1992) 48(4) Journal of Social Issues 161 on the dimensions of trust.

[279] Interview 13.

[280] Interview 3.

We should not overstate the extent to which Cloud Investigations can reassure customers in reality. It is outside of the scope of this paper to analyse this point fully. However, generating trust or re-establishing trust[281] in cases of distrust depends on a complex mix of factors including customer awareness (e.g. of the Cloud Investigation and its outcomes), and individual customer traits (e.g. the extent to which they are anxious or ill-at-ease with the operations of a specific Cloud Provider). In the words, a former employee of one of the EU DPAs:

> '… we can all live in a bit of a fishbowl here [when a Cloud Investigation is being conducted], where we might have the sense that - and I speak as much [from] the regulator in this respect. We might have a sense that everybody is watching and that everybody is going to be influenced by the outcome of the [Cloud Investigation].
>
> I'm not sure if that's the case. Actually, I think if there was a very negative [Cloud Investigation], I think people would certainly reflect on that. But in general, providing things are relatively okay, I don't think users pay that much of attention to it.'[282]

Secondly, Cloud Providers are often motivated to be open and transparent (subject to the above caveat) with EU DPAs during Cloud Investigations to avoid a binding decision being taken against them.[283] According to some of our respondents, this has been a more prominent motivation since the ruling of the Grand Chamber of the Court of Justice of the European Union ('CJEU') in *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González* ('*Google Spain*').[284] In *Google Spain*, Mario Costeja González, a Spanish national, made a complaint to the Spanish Data Protection

---

[281] Re-establishing trust after distrust has set in is an even more arduous task depending on factors including whether the self-perpetuating cycle of distrust can be brought to an end. For more on the difficulties of overcoming distrust, see T Govier, 'Distrust as a practical problem,' (1992) Journal of Social Philosophy, 23.

[282] Interview 12

[283] E.g. Interviews 1, and 3.

[284] Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos (2014)* <http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd7a8d4de5f8924b8981908f4c6ceda6bb.e34KaxiLc3qMb40Rch0SaxuPb3z0?text=&docid=153853&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=53717> accessed 10 February 2015.

Agency ('AEPD') against La Vanguardia newspaper, Google Spain and Google Inc., in relation to pages in the newspaper which appeared in Google search results when his name was searched for. The pages contained an announcement for a real estate auction following proceedings for the recovery of social security debts owed by Mr Costeja González. The AEPD rejected the claim against La Vanguardia as the information had been lawfully published by it, but upheld the complaint against both Google entities and requested that they take the necessary measures to withdraw the personal data from their indexes. Google Spain and Google Inc. brought actions before the Spanish High Court seeking to have the AEPD decision annulled. The Spanish High Court referred the matter to the Court of Justice of the European Union ('CJEU') under the preliminary ruling procedure. One of key aspects of the *Google Spain* ruling is that the CJEU found that Google Inc. – which was physically located in the United States of America – was established for data protection purposes in Spain due to the 'inextricable links' between the activities of Google Inc. and Google Spain.[285] In effect this means that Google Inc. is potentially subject to the data protection laws of every European jurisdiction where it has similar 'inextricable links.' According to our respondents, the Google Spain judgment was partly due to the unwillingness of Google Inc. to implement the recommendations of various EU DPAs following their investigations of the amended privacy policy of Google Inc.[286] Although many EU DPAs have fined Google after their investigation, Google still did not implement the changes.[287] Thus, the *Google Spain*

[285] Ibid. Para 55

[286] E.g. Interviews 1 and 3. Following Google Inc.`s ('Google') consolidation of the privacy policies, applicable to sixty Google services into one single document, various investigations were triggered against Google in Europe. Examples include the A29WP-mandated and the French DPA`s investigations. Such investigations found that Google`s consolidated privacy policy breached the relevant data protection laws and made a number of recommendations which Google refused to implement. For more on this see A29WP, Google Privacy Policy: Main Findings and Recommendations (16 October 2012) < http://www.cnil.fr/fileadmin/documents/en/GOOGLE_PRIVACY_POLICY-_RECOMMENDATIONS-FINAL-EN.pdf> accessed 16 July 2014; Letter from A29WP to Google (16 October 2012) < http://dataprotection.ie/documents/press/Letter_from_the_Article_29_Working_Party_to_Google_in_relation_to_its_new_privacy_policy.pdf> accessed 16 July 2014 and decision No. 2013-025 on 10 June 2013 by the Chair of the Commission Nationale de l`Informatique et des Libertes giving formal notice to the company Google Inc.

[287] E.g. Agencia Espanola de Protectione des Datos, 'The AEPD sanctions Google for serious violation of the rights of the citizens,' (Press Release, 20 December 2013) <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/diciembre/131219_PR_AEPD_PRI_POL_GOOGLE.pdf> accessed 12 July 2014.

judgment has been viewed by many EU DPAs[288] and Cloud Providers[289] as a strategy deployed to unequivocally emphasise to Google Inc. that it would not be able to evade European data protection laws.

As one of our respondents says:

> '…you take a company that has not been co-operative generally, Google, they are now waking up to the consequences of that approach. You get an ECJ judgment that says that you are subject to every EU DPAs, and gives you, to be fair to Google, a horrible job to be done in terms of dealing with deletion requests. So the rest of the multinationals can see that not playing ball with the regulator is extremely bad for business. Google of course still makes a lot of money. But in terms of reputation, it is seriously suffering.'[290]

Thus, since the *Google Spain* judgment, many big Cloud Providers are keener to co-operate and interact more with EU DPAs during Cloud Investigations[291] to prevent (as much as possible) EU DPAs from escalating matters. The desire to avoid the '…production of citable materials'[292] – which mean a court ruling which settles specific questions, such as whether an EU DPA has jurisdiction over the activities of a multinational Cloud Provider – is a key motivation for some Cloud Providers to co-operate more fully with EU DPAs during Cloud Investigations even where the EU DPAs may arguably not have jurisdiction over their activities.[293] For example, in one Cloud Investigation, the EU DPA was unsure whether it had jurisdiction over the Cloud Provider.[294] During the preliminary stages of the Cloud

[288] E.g. Interviews 1 and 3.

[289] E.g. Interviews 10, 11, 12, 13.

[290] Interview 1.

[291] E.g. interview 3

[292] Interview 3

[293] Interview 3.

[294] Interview 3.

Investigation, the Cloud Provider raised this point.[295] The EU DPA informed the Cloud Provider that it would refer the question to the national courts if the Cloud Provider kept questioning its authority.[296] The Cloud Provider 'kept talking' to the EU DPA to resolve its data protection concerns.[297] 'They [Cloud Providers] like to keep this uncertainty' rather than having a ruling which is similar in effect to the *Google Spain* judgment.[298] Such Cloud Providers here prefer to avoid binding decisions to avoid reputational damage as well as the financial cost of having to bring their operations and policies in line with the relevant data protection laws in cases where the courts rule that the EU DPA has jurisdiction over the Cloud Provider.

Thirdly, normative considerations invariably also influence how Cloud Providers behave during Cloud Investigations. Our data analysis shows that these normative motivations do not operate in a vacuum but are often interlinked with other considerations, such as economic ones. As always the 'what' and 'how' of such interactions are context-specific. We illustrate this point by exploring two behavioural patterns of two specific Cloud Providers during two Cloud Investigations. Our first Cloud Provider is motivated by normative concerns during Cloud Investigations in the sense of recognising the legitimacy[299] of European data protection laws. It thus has '…an overall policy of fully cooperating with [European] data protection authorities because we fully recognise the important position that they have in relation to enforcing the rights [that they have] within Europe (sic).'[300] Its approach can be explained by the fact that the Cloud Provider has been trading in Europe for over three decades. Consequently, this Cloud Provider has been interacting with EU DPAs for a long time in the context of its European activities and has not disputed their jurisdiction over its activities.[301] This Cloud Provider also recognises that the EU DPA, which is currently

[295] Ibid.

[296] Ibid.

[297] ibid

[298] Interview 3

[299] Legitimacy means [●].

[300] Interview 12

[301] Interview 12.

investigating it, has 'strong powers' of investigation,[302] such as the power to conduct on-spot inspections, search premises and seize equipment without a judicial warrant. Consequently, the EU DPA '…ha[s] to be given every cooperation.'[303] Moreover, the 'open'[304] and co-operative attitude of this Cloud Provider during this Cloud Investigation can also be explained by its business model which does not involve monetising the personal data of its users. Therefore, this Cloud Provider feels that '…'[its] privacy story is one that we can be open about' as its business model does not involve 'commodifying'[305] its users` personal data.[306]Here specific normative and commercial considerations impact on their behaviours towards EU DPAs Cloud Investigations ('Scenario A).

Our second Cloud Provider is also motivated by normative and economic concerns during Cloud Investigation ('Scenario B'). However, these concerns and their interconnections are different from the ones present in Scenario A. The Cloud Provider in Scenario B is motivated to co-operate as fully and openly as possible (subject to the usual caveat) with the EU DPA during its current Cloud Investigation because this EU DPA will be the main regulator for its European operations.[307] Consequently, this Cloud Provider is willing to invest its time and resources to fully (subject to the usual caveats) engage in the Cloud Investigation for various reasons including establishing a productive working relationship with the EU DPA, educating the EU DPA about its operations and policies, ascertaining to what extent it complies with the relevant data protection laws of a jurisdiction where it has recently relocated to, and avoiding the deployment of formal procedures by the EU DPA (e.g. formal adjudication of a complaint by a data subject). [308]

---

[302] Interview 12

[303] Interview 12

[304] Interview 12

[305] This refers to the process of turning personal data in commodities which can be traded by the data controllers to other parties, such as advertisers, for the purposes of making a profit.

[306] Interview 12

[307] Interview 11

[308] Interview 11. Some of our respondents (Cloud Providers) are also keener to establish a productive relationship with the EU DPA during the Cloud Investigation given that they will have far more onerous obligations to fulfil if and one the new regulation is deployed. Here responsiveness is deployed as a

Having examined the multiple compliance attitudes of Cloud Providers during Cloud Investigations, such as strategic openness and collaboration with EU DPA to generate trust with their customers or avoid a binding decision, next we examine why Cloud Investigations are being increasingly deployed in Europe.

4 Explaining the Growth of Cloud Investigations and Potential Limitations

In this section, we underline three reasons why Cloud Investigations are being increasingly deployed by EU DPAs.[309] As fully explored in the preliminary D-4.11, on a numerical level, since 2011, there has been a steady rise of Cloud Investigations conducted by various EU

pro-active strategy to foster an effective relationship with the EU DPA which, for example, enables them to ask the EU DPA for advice about their further obligations when the new Regulation is enacted. Interview 7.

[309] There are no official quantitative estimates of the number of Cloud Investigations conducted by EU DPAs. The notion that Cloud Investigations are become more frequent in Europe is derived from our documentary and interview analysis. Our interviewees have told us that Cloud Investigations are being more frequently carried out since the past few years (e.g. interviews 1, 2, 3, 4). Additionally, an extensive Google search conducted for the preliminary D-4.11 has shown that EU DPAs are investigating more and more Cloud Providers since 2011. We chose 2011 as the starting point from which to track cloud investigations in Europe we could not find evidence of cloud investigations conducted by European DPAs before that date. This can be explained by several factors including the lack of penetration of cloud computing services in the European market before 2011. It should also be noted that not all Cloud Investigations conducted by EU DPAs are reported in the press (e.g. Interviews 3, 4 and 5) and at times even if an EU DPA has investigated a Cloud Provider it may not always admit it has done so for various reasons such as political sensitivities (e.g. Interview 3). Consequently, we do not propose to provide a quantitative estimate of the notion that Cloud Investigations are being more frequently deployed in Europe. For our purposes, we support our assumption by relying on our documentary and interview analysis. Examples of Cloud Investigations in Europe include the investigation of Facebook Ireland Ltd by the Irish DPA – see Data Protection Commissioner of Ireland, 'Report of Audit of Facebook Ireland Limited,' (21 September 2011) <http://dataprotection.ie/documents/facebook%20report/final%20report/report.pdf> accessed 12 September 2014, the joint investigation of WhatsApp Inc by the Dutch and Canadian DPAs – see Dutch Data Protection Authority, 'Report on the Definitive Findings of the Investigation into the Processing of Personal Data for the WhatsApp Mobile Application by WhatsApp Inc,' (January 2013) <http://www.google.co.uk/url?sa=t&rct=j&q=WHATSAPP+DUTCH+DPA+REPORT&source=web&cd=2&ved=0CCsQFjAB&url=http%3A%2F%2Fwww.dutchdpa.nl%2Fdownloads_overig%2Frap_2013-whatsapp-dutchdpa-final-findings-en.pdf&ei=cdwSVPwJg-Zo0pKB6Ag&usg=AFQjCNFqJFjvUqFPWy3pZJwX6FdMJ9dxWQ&sig2=n2m10rQ6A1u13QolOL7skQ> accessed 12 September 2014, the investigation of Google Inc.`s amended privacy policy by various EU DPAs – see A29WP, Google Privacy Policy: Main Findings and Recommendations (16 October 2012) < http://www.cnil.fr/fileadmin/documents/en/GOOGLE_PRIVACY_POLICY-_RECOMMENDATIONS-FINAL-EN.pdf> accessed 16 July 2014; Letter from A29WP to Google (16 October 2012) < http://dataprotection.ie/documents/press/Letter_from_the_Article_29_Working_Party_to_Google_in_relation_to_its_new_privacy_policy.pdf> accessed 16 July 2014.

DPAs, such as the Irish DPA and the Bavarian DPA.[310] We also argue that the effectiveness of Cloud Investigations as regulatory tools can be hampered by the degree to which the regulatory process is generated as an 'arranged production of information' which sheds specific views on certain aspects of compliance rather than all aspects of compliance.[311]

4.1 Accounting for More Frequent Cloud Investigations

Firstly, one could argue that the growing number of Cloud Investigations in Europe is not surprising as cloud-based services and applications are gradually proliferating in various sectors in Europe.[312] Having said that, all of our EU DPA respondents have stressed that none of the companies which they have investigated or are currently investigating have been targeted merely because they are using and/or offering cloud computing services and/or technologies to their customers.[313] Rather, as the technologies and services offered by Cloud Providers have become more popular in Europe, there has been a concurrent increase in the data protection issues raised by such companies.[314] Consequently, when many EU DPAs plan their inspection agenda for a forthcoming inspection period, they consider whether such companies should be investigated as '…there's a certain demand to know what is going on, and the only way to find out what is really going on is to ask and demand that the questions are being answered.'[315]

The media furore which has accompanied the investigations of multinational Cloud Providers (e.g. Facebook, LinkedIn and Google) by EU DPAs illustrate that these investigations can often receive a high level of publicity.[316] Some of our respondents argue that extensive publicity means that Cloud Investigations can often be effective strategies

---

[310] See Section 3 of the preliminary D-4.11 (n 3) for more.

[311] n 61.

[312] E.g. Interviews 2, 3. Recent figures estimate that the Europe cloud market will be worth nearly €80 billion by 2020 <https://ec.europa.eu/digital-agenda/en/about-cloud-computing> accessed 10 February 2015.

[313] E.g. Interviews 1, 2, 3.

[314] Ibid.

[315] Interview 14.

[316]

deployed by some EU DPAs to address the historic concern that they are 'toothless.'[317] For many of our EU DPA respondents, the spectre of the 'toothless watchdog' often still looms at the horizon.[318] The spectre can cast even longer shadows in cases where multiple stakeholders (e.g. NGOs, other non-EU DPAs[319], and the media) vigorously question whether the scope of a Cloud Investigation is wide enough to enable the EU DPA to evaluate all the relevant processing operations and policies of the Cloud Provider. Here, the investigative process becomes a significant strategy through which the relevant EU DPA '…is seen to be proactively addressing privacy concerns rather than simply being a light touch.'[320] Arguably, not all Cloud Investigations attract a similar level of media and public interest.[321]

Secondly, as many multinational Cloud Providers increase their European user-base, they often designate one specific European member state as the country of their 'establishment' for data protection purposes.[322] Consequently, some EU DPAs opt to proactively investigate whether the activities of such Cloud Providers comply with the relevant data protection laws rather than await to react merely when potential data protection issues or complaints arise.[323]

---

[317] Many EU DPAs, such as the UK DPA, have been labelled as 'toothless' when exercising their data protection powers. See J A Cannatacia and P M Bonnicib, 'The UK 2007–2008 data protection fiasco: Moving on from bad policy and bad law?,' (2009) 23(1) International Review of Law, Computers and Technology 47; D H Flaherty, 'The emergence of surveillance societies in the western world: Toward the year 2000, (1988) 5(4) Government Information Quarterly, 377, 383.

[318] E.g. Interviews 1, 2, 3, 4, 14.

[319] E.g. In one of its current Cloud Investigations, one EU DPA has to take into account the data protection concerns of a non-EU DPA as the Cloud Provider in question has indicated that its branch – located in this EU DPA`s jurisdiction – is the 'data controller' for the purposes of its operations in the non-EU DPA`s jurisdiction. Interview 1.

[320] Interviews 11. Also Interview 4.

[321] Interview 12.

[322] E.g. Interview 1. Under Article 4(1) of the DPD (n 7), the DPD only imposes obligations on data controllers that fulfil the establishment criteria as set out in Article 4(1)(a) to (c).

[323] E.g. Interviews 1 and 12.

Thirdly, Cloud Investigations are more regularly utilised as regulatory tools by EU DPAs because they often achieve 'better end results' than other regulatory tools, such as lawsuits[324] for the EU DPA and Cloud Provider. Better end results for EU DPAs mean a systematic and lasting change in the conduct, processes, and policies of the Cloud Provider.[325] For Cloud Providers, better end results mean that their activities comply with the relevant data protection laws with minimal damage to their business model or reputation.[326] Compared to other regulatory tools, such as litigation, Cloud Investigations can achieve better end results for the EU DPA and Cloud Providers because they are, to varying degrees, wider in scope, less formal, and enacted through regular and less formal interactions between the parties over a long period of time.[327] In terms of scope, other regulatory tools, such as lawsuits, are narrower in scope than Cloud Investigations as they invariably focus on a set of narrow data protection issues. However, during a Cloud Investigation, where appropriate (e.g. resources, expertise), the EU DPA can evaluate all the relevant aspects of the Cloud Provider`s processing operations and policies.[328]

In particular, as Cloud Investigations Cloud Investigations are enacted through various informal interactions between EU DPAs and Cloud Providers (e.g. email, conference calls, face to face meetings in informal settings) over a sustained period of time, this can often lead to two interconnected advantages for the EU DPA and Cloud Provider. In the first place, for some EU DPAs, that are the competent regulator for the European operations of Cloud Providers, Cloud Investigations are useful regulatory tools which enable them to gain in-depth knowledge about its regulatees. Such EU DPAs would struggle to effectively oversee the operations of such Cloud Providers if they did not know the organisation in detail. [329] Moreover, as the EU DPAs carry on engaging with the Cloud Provider after the Cloud Investigation (e.g. to oversee how the Cloud Provider implements its

[324] E.g. Interviews 1, 2, 3, 4.

[325] Ibid.

[326] E.g. Interview 10, 11, 12,13

[327] n 253.

[328] Interview 1.

[329] Interview 1.

recommendations or discuss the data protection issues raised by the Cloud Provider`s future technologies), they can often address data protection issues 'upfront' (i.e. proactively) rather than wait till a complaint is filed.[330]

In the second place, as Cloud Investigations can often involve extensive rapport-building, some EU DPAs and Cloud Provider can develop more positive relationships during this regulatory process than they would in other regulatory processes (e.g. lawsuit).[331] Far from the confrontational court room setting, the parties can often reach an agreement during the Cloud Investigation which leads to a 'deep change' in how the company processes personal data (e.g. the type of personal data it processes) at minimal costs to its business model or reputation.[332] Here this fundamental change in the operations and policies of the company is often linked to the fact that the EU DPA continues 'talking to' the company after the Cloud Investigation.[333] However, as examined in sections 3.3 and 3.4, the outcomes of Cloud Investigations are very much context-specific. Consequently, at times, as compliance responses or regulatory styles change, the relationships between the Cloud Provider and EU DPA can shift from a pollyanistic to a '…David versus Goliath' type relationship.[334] Some of our EU DPA respondents underline that many multinational Cloud Provider tend to be less unresponsive during the Cloud Investigations since the Snowden revelations and the Google Spain ruling.[335]

Having explored three of the main reasons why Cloud Investigation are more frequently deployed by EU DPAs, next, we analyse how one additional factor (other than those examined in section 3), namely, the extent to which specific realities are constructed during Cloud Investigations, can limit the effectiveness of Cloud Investigations as 'regulatory tools'.

---

[330] E.g. Interviews 10 and 11.

[331] E.g. n 251.

[332] E.g. Interview 1.

[333] E.G. Interview 1

[334] Interview 3.

[335] E.g. Interviews 1 and 3.

4.2 Constructing Realities during Cloud Investigations

Our interview data analysis emphasises interesting distinctions between Cloud Investigations as a reality and Cloud Investigations as an ideal. In an ideal world, the EU DPA would investigate all the relevant processing operations and policies of the Cloud Provider.[336] However, in reality, several factors can impede the scope and extent of Cloud Investigations. In particular, during some Cloud Investigations, many EU DPAs can often only see what the Cloud Provider '…wants to show to [them]'[337]. For example, some EU DPAs only check specific portions of algorithms to assess the security measures which apply to specific processing operations.[338] This consists of reading the algorithmic sequences provided by the Cloud Provider for logical consistency.[339] In other cases, some EU DPAs test specific portions of algorithms to determine whether their output matches the logic, for example, the retention period of a specific cookie.[340] As with the previous example, the EU DPA here obtains the relevant sequence from the Cloud Provider and has to trust that this algorithmic sequence is the one that is actually implemented by the Cloud Provider.[341]

This dichotomy between the idealised view of the Cloud Investigation and its reality may not always be apparent to the data subject or other stakeholders (e.g. general public) who may assume that the EU DPA obtains a 'fully accurate picture'[342] during the Cloud Investigation. For example, during a recent Cloud Investigation, the EU DPA in question did not examine the data protection issues raised when this Cloud Provider shared information about the interactions of suspected paedophiles on its websites with the law enforcement

[336] E.g. Interviews 3 and 9.

[337] Interview 9

[338] Interview 3

[339] Ibid.

[340] E.g. Our analysis of several investigations reports published by the EU DPAs which participated in Interviews 1, 2, 3, 4, 14. We cannot list the reports as this would disclose the identities of our respondents.

[341] E.g. Interview 1.

[342] Interview 9

authorities of two European jurisdictions.[343]At the time of this Cloud Investigation, other stakeholder (e.g. other EU DPAs etc) were unware of this practice as it only '…popped up in the news' two months after the conclusion of this Cloud Investigation.[344] It could have been the case that either the Cloud Provider itself did not inform the EU DPA of this practice or that as part of the bartering between the two parties during the Cloud Investigation, the EU DPA agreed not to include this in its public report for political reasons.[345] Either way, this illustrates the potentially wide gap between Cloud Investigations in practice and in theory and how Cloud Investigations can be represented in specific ways by the Cloud Provider and EU DPA so that only a partial view is shed on the compliance of the Cloud Provider with the relevant data protection laws. As one of our respondents emphasises repeatedly: '…All this you don't see. All this you don't see.'[346] These partial views of compliance may often be crafted by the EU DPA and Cloud Provider when the findings of the Cloud Investigation are published.[347]

This is a key limitation of Cloud Investigations which, if unaddressed, would impede its effectiveness as one of the mechanisms through which Cloud Providers provide accounts of its compliance with relevant laws to an independent regulatory body.[348]

5 Conclusion

In this deliverable we have argued four points. Firstly, Cloud Investigations are complex regulatory processes that often involve different co-operative relationships between various actors, such as DPAs operating across many jurisdictions. In practice, manifold interactions

[343] Interview 9.

[344] Interview 9.

[345] Interview 9.

[346] Interview 9.

[347] Interview 9.

[348] It is beyond the scope of this paper to analyse the concept of accountability at length. See MS:C-2.2 'Conceptual Framework' (A4 Cloud). Accountability has other facets such as rendering specific accomplishments visible to specific audiences, and rectification. We will make more explicit links between accountability and Cloud Investigations in our May Deliverable and April Report.

and practices, such as facilitative instruments, are deployed to form and perform such collaborations which are significant to ensure the consistent application and enforcement of common data protection principles in an increasingly globalised context. Complexity can also manifest itself through several factors, such as budgetary constraints and pressures from stakeholders including the press, which impact on key aspects of Cloud Investigations. How such complexities are resolved during Cloud Investigations can often involve intricate and context-specific strategies, such as delegating action to a third-party. Secondly, regulation through Cloud Investigation is dynamic as it involves constant activities from multiple actors, continually evolving regulatory styles and compliance attitudes. This means that the regulatory encounters between Cloud Providers and EU DPAs during an investigation often involve ceaseless change. Thirdly, Cloud Investigations can, at times, be contested as EU DPAs and Cloud Providers attempt to resist each other`s attempts to direct the investigation in particular ways. Finally, we have argued that three reasons including the benefits of rapport-building, and relocation of some of the operations of multinational Cloud Providers to Europe, can account for why Cloud Investigations are growing in frequency in Europe. Here we have also underlined how the construction of specific realities during some Cloud Investigations (e.g. compliance attitudes) can hamper the effectiveness of Cloud Investigations as regulatory tools in the sense of enforcing all the relevant data protection laws. Interestingly, our data analysis also shows that the rhetoric surrounding Cloud Investigations (e.g. during investigation reports, press releases or our own interviews) does not as yet explicitly bring in the technical considerations underpinning the cloud, such as how different cloud models (e.g. IaaS and SaaS) can raise data control and security issues to varying degrees.[349] As more Cloud Providers are investigated, with distinct offerings targeted at both individual and corporate users, it would be interesting to determine whether such investigations become more focussed on specific technical considerations in the cloud.

[349]Jatinder Singh, et al, 'Regional clouds: technical considerations,' University of Cambridge, Computer Laboratory, Tech. Rep. UCAM-CLTR-863 (2014).

6 References

Ayeres I and Braithwaite J, *Response Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992)

Baier A C, 'Trust and antitrust,' (1986) 96(2) 231

Baldwin R and Cave M, *Understanding Regulation* (Oxford University Press 1999)

Baldwin, Robert, Cave Martin, and Lodge Martin, Understanding *regulation: theory, strategy, and practice* (Oxford University Press 2012)

Bennett Colin J, 'Privacy advocacy from the inside and the outside: Implications for the politics of personal data protection in networked societies,' (2011) 13(2) Journal of Comparative Policy Analysis 125

Bennett Colin J, *Regulating privacy: data protection and public policy in Europe and the United States* (Cornell University Press 1992)

Black Julia, 'Enrolling actors in regulatory systems: Examples from UK financial services regulation,' (2003) Public Law 63

Black Julia, 'Critical reflections on regulation,' (2002) 27 Austl. J. Leg. Phil. 1

Braithwaite Valerie et al, 'Regulatory Styles, Motivational Postures and Nursing Home Compliance,' (1994) 16(4*) Law & Policy* 363

Brownsword and K Yeung, 'Regulating Technologies: Tools, Targets and Thematics' in Brownsword R and Yeung K, (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart 2008)

Bryman Alan, *Social Research Methods* (OUP 2012)

Bygrave Lee A, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002)
Carey P, *Data Protection: A Practical Guide to UK and EU Law* (OUP 2011)

Cavoukian A and Tapscott D, *Who Knows: Safeguarding your Privacy in a Networked World* (Random House Toronto 1995)

Cotterrell Roger, *Law's Community: Legal Theory in Sociological Perspective* (Clarendon Press 1997)

Crouch Mira, and McKenzie Heather, 'The logic of small samples in interview-based qualitative research,' (2006) 45(4) Social science information 483

Galligan Denis, *Law in Modern Society* (Oxford University Press 2007)

Gerson Kathleen and Horowitz Ruth, 'Observation and interviewing: Options and choices in qualitative research,' (2002) Qualitative research in action 199

Govier T, 'Distrust as a practical problem,' (1992) 23 Journal of Social Philosophy 52

Grasmick Harold G and Bursik RJ Jr. 'Conscience, significant others, and rational choice: Extending the deterrence model,' (1990) Law and society review (1990) 837

Guba GE and Lincoln YS, 'Competing paradigms in qualitative research,' (1994) 2 Handbook of Qualitative Research 163

Gunningham N, 'Enforcement and compliance strategies,' in Baldwin Robert, Cave Martin, and Lodge Martin (eds) *The Oxford Handbook of Regulation* (OUP 2010) 120

Hood Christopher, 'Intellectual obsolescence and intellectual makeovers: reflections on the tools of government after two decades,' (2007) 20(1) Governance 127

Hood Christopher, *The Tools of Government* (London Macmillan 1983)

Hon W Kuan, Millard Christopher, and Walden Ian, 'What is Regulated as Personal Data in Millard Christopher (ed) *Cloud Computing Law* (Oxford University Press 2013)
Hon W Kuan, Millard Christopher, 'Cloud Technologies and Services,' in Millard Christopher (ed) *Cloud Computing Law* (Oxford University Press 2013)

Hutter B, 'Regulating Employers and Employees: Health and Safety in the WorkPlace,' (1993) Journal of Law and Society 452

Jackson Howell E, 'Variation in the intensity of financial regulation: Preliminary evidence and potential implications,' (2007) 24 Yale J. on Reg. 253

Jolls Christine, Cass R Sunstein, and Thaler Richard, 'A behavioral approach to law and economics,' (1998) Stanford Law Review 1471

Kasperson R E, Golding D, & Tuler S, 'Social distrust as a factor in siting hazardous facilities and communicating risk,' (1992) 48(4) Journal of Social Issues 161

King N and Horrocks C, *Interviews in qualitative research* (Sage 2010)

Kuner Chris, *Transborder Data Flows and Data Privacy Law* (OUP 2013)

Kuner C, 'An international legal framework for data protection: Issues and prospects,' (2009) 25(4) Computer Law & Security Review 307

Lange Bettina, 'Compliance construction in the context of environmental regulation,' (1999) 8(4) Social & Legal Studies 549

Latour Bruno, *Reassembling the Social. An Introduction to Actor-Network-Theory* (Oxford University Press 2005)

Latour Bruno, 'The Powers of Association' in John Law (ed) *Power, Action and Belief: a New Sociology of Knowledge?* (London Boston and Henley, Routledge and Kegan Paul 1986)

Lessig Lawrence, *Code 2.0* (Basic Books 2006)

Lessig Lawrence, 'Privacy and Attention Span,' (2000) 89 Geo. Lj 2063

Lodge, Martin, Kai Wegrich, and Gail McElroy, 'Dodgy kebabs everywhere? Variety of worldviews and regulatory change,' (2010) 88(1) Public Administration 247

Lynskey O,' Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order,' (2014) 63(3) International and Comparative Law Quarterly, 63(03), 569

May Peter, and Winter Soren, 'Reconsidering Styles of Regulatory Enforcement: Patterns in Danish Agro-Environmental Inspection,' (2000) 22(2) Law & Policy 143

McGeveran William, 'Programmed Privacy Promises: P3P and Web Privacy Law,' (2001) 76 NYUL Rev. 1812

Murray Andrew D, 'Conceptualising the Post-Regulatory (Cyber)State' in Yeung Karen and Brownsword Roger (eds) *Regulating technologies: legal futures, regulatory frames and technological fixes* (Hart 2008) 287

Murray Andrew D, *The Regulation of Cyberspace: Control in an Online Environment* (Routledge Cavendish 2006)

Pearson Siani and Benameur Azzedine, 'Privacy, security and trust issues arising from cloud computing,' (IEEE Second International Conference on Cloud Computing Technology and Science, 2010)

Poullet Yves, 'EU data protection policy. The Directive 95/46/EC: Ten years after,' (2006) 22(3) Computer Law & Security Review 206

Raab Charles D, 'Networks for Regulation: Privacy Commissioners in a Changing World,' (2011) 13(2) Journal of Comparative Policy Analysis 195

Raab Charles D, 'Information privacy: networks of regulation at the subglobal level,' (2010) 1(3) Global Policy 291

Raab Charles D, 'Co-producing Data Protection,' (1997) 11(1) International Review of Law, Computers & Technology 11

Raab CD and De Hert P, 'The Regulation of Technology: Policy Tools and Policy Actors,' in (ed) Yeung K and Brownsword R, *Regulating technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart 2008)

Raab Charles D and Koops Bert-Jaap, 'Privacy actors, performances and the future of privacy protection,' in Gutwith Serge et al (eds) *Reinventing Data Protection?* (Springer 2009)

Raskolnikov Alex, 'Revealing Choices: Using Taxpayer Choice to Target Tax Enforcement,' Columbia Law and Economics Working Paper No. 337 (11 February 2009) <http://ssrn.com/abstract=1267622> accessed 10 February 2015

Reed C, *Making Laws for Cyberspace* (OUP, 2012)

Singh Jatinder et al, 'Regional clouds: technical considerations,' University of Cambridge, Computer Laboratory, Tech. Rep. UCAM-CLTR-863 (2014)

Sjaak Nouwt, 'The Role of Data Protection Authorities,' in Poullet Yves, De Hert Paul, and De Terwangne Cécile (eds) *Reinventing data protection?* (Springer 2009) 136

Stafford Sarah L, 'Self-policing in a targeted enforcement regime,' (2008) Southern Economic Journal 934

Strathern Marilyn, 'Abstraction and decontextualisation: an anthropological comment or: e for ethnography' (Undated Pre-Publication Draft) <http://virtualsociety.sbs.ox.ac.uk/GRpapers/strathern.htm> accessed 10 February 2015

Vaquero Luis M et al, 'A break in the clouds: towards a cloud definition,' (2008) 39(1) ACM SIGCOMM Computer Communication Review 50

Vranaki A and Reed C, 'The Rise of Investigations by European Data Protection Authorities in the Context of Cloud Computing,' (A4 Cloud, WP 44, D-4.11, 30 September 2014)

Warren C A B, 'Qualitative Interviewing,' in Gubrium J F and Holstein J A (eds) *Handbook of Interview Research: Context and Method* (Thousand Oaks CA Sage 2002)

Wouter Poortinga and Pidgeon Nick F, 'Exploring the dimensionality of trust in risk regulation,' (2003) 23(5) Risk analysis 961

Yin Robert K, *Qualitative Research: Design and Methods* (Sage 2013)

.