4 Legal uncertainty under the Protection of Personal Information Act during the pandemic

Exploring European case law as an interpretive guideline

Jonas S Baumann* , Nazreen Ismail**

Faculty of Law,
University of Johannesburg

Abstract

In early 2020, the COVID-19 virus rapidly spread around world and forced people to significantly adjust their lives. Lockdowns compelled society to digitalise, thereby substantially increasing the processing of personal information. On 17 June 2020, when South Africa faced the pandemic's "first wave", key provisions of the Protection of Personal Information Act 4 of 2013 (POPIA) were enacted from 1 July 2020, further enabling full enforcement from 1 July 2021. This first South African omnibus data protection act unleashes legal uncertainty due to the highly abstract formulation of its provisions. Considering the recent increase of processing of personal information, the "young" POPIA is under pressure to evolve quickly to mitigate liability risks for responsible parties and at the same time provide a reliable and predictable framework ensuring the protection of protection of personal information.

As a possible approach to increase legal certainty, this chapter will explore the adoption of European data protection case law when

* Dipl-Jur (Saarland University), LLM (UJ). Research Associate, Research Centre for Private International Law in Emerging Countries at the University of Johannesburg.

** LLB, LLM (UJ). Lecturer: Department of Practical Business Law at the University of Johannesburg. Attorney of the High Court of South Africa.

interpreting the POPIA taking into account recent decisions of the South African Constitutional Court. Since the 1995 EU Data Protection Directive was used as an integral source when drafting the POPIA, this approach appears to be promising and could potentially contribute to a rapid increase of legal certainty in the *terra incognita* of South African data protection law. The adoption of European case law will be examined in the context of three fundamental concepts of data protection law namely, personal information, joint responsibility and consent.

1 Introduction

On 17 June 2020, when South Africa stood at the beginning of the pandemic's "first wave", President Cyril Ramaphosa paved the way for a new "era"[1] of South African data protection law by proclaiming the applicability of key provisions of the Protection of Personal Information Act[2] (POPIA) from 1 July 2020,[3] hereby enacting a compliance deadline until 1 July 2021.[4] This act, which was gazetted in 2013,[5] is the first omnibus data protection act in the Republic. Considering the timing of its commencement, the POPIA could be described as a "child of the pandemic". The POPIA aims to give effect to the constitutional right to privacy[6] and allows the information regulator to impose fines and issue other orders against responsible parties[7] that do not comply with its legal framework.[8]

The pandemic forced society to digitalise, thereby significantly increasing the processing of personal information. The national lockdowns resulted in the closing of schools, universities and offices which forced many sectors to work remotely and rely heavily on video conferencing services and cloud providers.[9] The number of users

1 *Cf* Baumann and Ismail "The concept of "personal information" in the Protection of Personal Information Act 4 of 2013—a comparative analysis from a European perspective" 2021 *TSAR* 718 719.
2 Act 4 of 2013.
3 Proclamation No R 21 of 2020, GG 43461 (22-6-2020) 3.
4 s 114(1) of the POPIA.
5 *GG* 37067 (26-01-2013).
6 s 2 of the POPIA.
7 The responsible party is the primary addressee of the Act, *cf* below 3.2.
8 See s 95(1) and s 109 of the POPIA.
9 On those developments *eg* Vester "Your business, the cloud, and lockdown" 30 April 2020 (https://businesstech.co.za/news/industry-news/393872/your-business-the-cloud-and-lockdown/ (8-1-2022)) and the ILO *Teleworking during the COVID-19 pandemic and beyond* (2020)

of social media platforms increased significantly.[10] Furthermore, technology has been utilised to fight the pandemic directly as COVID-19 tracing apps were launched to trace infection chains and warn people who possibly came in contact with infected persons, thereby raising privacy concerns in legal systems around the globe.[11] This sudden increase in the processing of personal information paired with other long term developments, such as the societal transformation within the Fourth Industrial Revolution, puts the POPIA under pressure to become operable and interpretable. In particular, the private sector requires a predictable and enhanced data protection framework to invest in and implement new technologies and business models. From this perspective, the *status quo* under the POPIA is rather sobering as the highly abstract formulations of the Act result in a significant degree of legal uncertainty. Numerous businesses and companies are financially drained by the impacts of the pandemic as well as the unrest which occurred during July 2021 in the provinces of Gauteng and KwaZulu-Natal.[12] As a result, they cannot afford legal uncertainty[13] which adds to the cost of data protection compliance[14] and the possible

---

2 f (https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/instructionalmaterial/wcms_751232.pdf (08-01-2022)).

10 The social network Facebook, for example, reported for the fourth quarter of 2020 an increase of 11 % of daily active users (year over year) compared to December 2019 (see the Facebook Reports Fourth Quarter and Full Year 2020 Results (27 Jan 2021) (https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/default.aspx (08-01-2022))).

11 On the data protection aspects of such applications see Bradford, Aboy and Lidell "COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes" 2020 *Journal of Law and the Biosciences* 1 ff; Lim "Assessing the implications of digital contact tracing for COVID-19 for human rights and the rule of law in South Africa" (2020) *AHRLJ* 540; Trotogott "A comparative analysis of data privacy impacted by Covid-19 contact tracing in the European Union, the United States and Israel: Sacrificing civil liberties for a public health emergency" 2020 *ILSA Journal of International & Comparative Law* 56 ff.

12 According to Reuters, the South African Treasury estimated the economic damage from the riots in Gauteng and KwaZulu-Natal in July 2021 to decrease the 2021 GDP by 0.7–0.9 percentage points (https://www.reuters.com/article/safrica-economy-idUSL8N2PV3RU (08-01-2022)).

13 Regarding the cost of legal uncertainty in general Wagner "Economic Analysis of Cross-Border Legal Uncertainty; The Example of the European Union" in Smits *The Need for a European Contract Law* (2005) 31 ff.

14 According to a survey by Datagrail, 34 per cent out of 301 involved companies employing more than 1000 employees spent more than US$ 1 million on the preparation of complying with the GDPR (Datagrail

cost of non-compliance.[15] Due to the recent enactment of the POPIA, case law on the interpretation of the provisions of the Act has rarely been reported[16] and the Information Regulator has not yet published policies and guidance notes addressing the interpretation of certain key concepts of the new South African data protection framework.[17] This creates an urgent need for the POPIA to evolve and become interpretable and operable.

The idea of adopting existing case law of the Court of Justice of the European Union (CJEU), in instances where the court already clarified the (autonomous)[18] interpretation of numerous provisions and concepts of the 1995 Data Protection Directive (DPD)[19] and its successor, the General Data Protection Regulation (GDPR),[20] could be a fruitful source to "add meat" onto the bony skeleton of the provisions of the POPIA. Therefore, it is not surprising, that this idea has already been introduced into the academic discussion on the POPIA.[21] This

---

The Age of Privacy: The Cost of Continuous Compliance (2020) 5 (https://datagrail.io/downloads/GDPR-CCPA-cost-report.pdf (08-01-2022)).

15 In the case of non-compliance with the POPIA, s 109(2)(c) provides for fines up to R 10 million. The GDPR provides for fines of up to € 20 million or 4 per cent of the total worldwide annual turnover of the preceding financial year of a company (see a 83(5) and (6) of the GDPR). In addition, both regimes provide for administrative measures by the data protection authorities and private enforcement instruments such as claims for damages by data subjects.

16 See eg *Divine Inspiration Trading 205 (Pty) Ltd v Gordon and Others* (22455/2019) 2021 (4) SA 206 (WCC) para 30 ff. (discussion of s 11 POPIA) and *Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others* (14867/20) [2020] ZAGPJHC 186 para 17 (where the court did not elaborate detail on the compliance of CCTV road surveillance with the POPIA).

17 Those documents are accessible via https://justice.gov.za/inforeg/docs.html (08-01-2022).

18 EU Law is to be interpreted autonomously and independently from member state law. See in general Martens *Methodenlehre des Unionsrechts* (2013) 335 ff; in context of EU data protection law CJEU, the *Planet49* case C-673/17 (2019) par 47.

19 Directive 95/46/EC of the European Parliament and of the Council (24-10-1995) on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, 31 ff.

20 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, 1 ff.

21 See Naude and Papadopoulus "Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments (2)" 2016 *THRHR* 213 228 introducing

idea deserves further exploration as it could increase the level of legal certainty in the South African data protection framework—not only during the pandemic. From a methodical perspective, South African courts are familiar with considering foreign case law to shape and clarify the South African legal framework. The question whether the case law of the CJEU can be adopted to interpret the provisions of the POPIA requires discussion,[22] as this omnibus data protection act introduced fundamental changes regarding the protection of privacy within the Republic.[23] Following this discussion, the adoption of landmark decisions of the CJEU as interpretive guidelines will be discussed in the context of three regulatory key concepts of the POPIA. The clarification of these concepts may provide a potential solution to mitigate legal uncertainty in the South African data protection framework which has been fuelled by the pandemic.[24]

2 The adoption of EU case law under the Protection of Personal Information Act

From a methodical perspective, the possibility to adopt CJEU case law in the field of data protection law when interpreting the POPIA requires further discussion. The role of the European data protection law in the interpretation of the POPIA is of particular relevance and will be discussed subsequently. Thereafter, recent judgments of the South African Constitutional Court will be discussed where minority judgments introduced several criteria for the potential reception of CJEU case law.

---

the idea of the adoption of the CJEU's decision in *Google Spain SL and Google Inc. v AEPD*, where the court introduced the so-called "right to be forgotten" under the DPD (CJEU, the *Google Spain* case C-131/12 par 89 ff.), in context of s 10 and s 24 the POPIA. See also Baumann and Ismail (n 1) 732 ff on the adoption of the *Breyer* judgment to interpret the term "personal information" under the POPIA. The latter will also be discussed below in par 3.1.

22 See below par 2.

23 Before the provisions of Act 4 of 2013 became applicable, the protection of privacy in South Africa was governed by established common law principles and claims (in detail Roos "Data Privacy Law" in Van der Merwe, Roos, Pistorius, Eiselen and Nel *Information and Communications Technology Law* (2016) 418 ff).

24 See below par 3.

2.1 The role of EU data protection law in the genesis of the Protection of Personal Information Act

The genesis of the Data Protection Bill and its final product, the POPIA, was a lengthy process.[25] During the course of this procedure, extensive reference was made to the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,[26] the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe[27] and the DPD.[28] The influence of the DPD on certain provisions of the POPIA is undeniable.[29] Several key provisions of the POPIA mimic the wording and systematisation of provisions contained in the DPD, evidencing the model-character of the European framework. For example, this applies to numerous definitions,[30] the material[31] and territorial scope rules,[32] the general principles of processing[33] as well as the grounds for processing.[34]

---

25 For the genesis of the POPIA, see Roos "Data Protection Law in South Africa" in Makulilo (ed) *African Data Privacy Laws* (2016) 201 ff; on the Data Protection Bill 2009: Makulilo *Protection of Personal Data in sub-saharan Africa* (2012 Thesis GER) 400 ff.

26 These principles have been revised in 2013 by the OECD Privacy Framework 2013; an overview on the guidelines is provided by Naude and Papadopoulus "Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments (2)" 2016 *THRHR* 213 219 ff.

27 Council of Europe, Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108/1981 from 28 January 1981; the convention has been revised in 2018: Council of Europe, Convention 108+ Convention for the protection of individuals with regard to the processing of personal data 2018.

28 See for example the references on those frameworks in the reform debate on the South African privacy and data protection law (SALRC, *Issue Paper 24 (Project 124)* (2003) sub 1.2.13 ff; SALRC, *Discussion Paper 109 (Project 124)* (October 2005) sub 1.2.13 ff.; SALRC, *Project 124 Privacy and Data Protection Report* (2009), sub 1.2.13 ff).

29 See for example the statement of Burns and Burger-Smidt, *A Commentary on the Protection of Personal Information Act* (2018) 8: "*…it becomes clear that the South African legislature relied heavily on the principles and objectives of the 1995 Directive in drafting the POPI Act*".

30 *e.g.* the concepts discussed below par 3.

31 See s 3(1)(*a*) of the POPIA and a 3 of the DPD.

32 See the territorial scope rule in s 3(1)(*b*) of the POPIA and a 4(1)(*a*) and (*c*) of the DPD. For a more detailed discussion of the territorial scope rules of the POPIA, the GDPR and the DPD see Baumann and Ismail "The (Extra-) territorial Scope Rules of the New European Data Protection Law from a Private International Law Perspective—A Model for South Africa?" 2021 (1) *CILSA* 8–17 and 30–34.

33 See s 8 ff of the POPIA and a 6 of the DPD.

34 See s 11 of the POPIA and a 7 of the DPD.

2.2 The adoption of European case law by the South African Constitutional Court

On several occasions in recent years, the South African Constitutional Court considered CJEU case law as an interpretive guideline. In *Horn v LA Health Medical Scheme*[35] as well as in *Rural Maintenance (Pty) Limited and Another v Maluti-A-Phofung Local Municipality*,[36] Zondo J, in his minority judgments, referred to CJEU case law when interpreting section 197 of the Labour Relations Act.[37] In both judgments,[38] Zondo J emphasised that section 197 was inspired by EU legislation.[39] This reasoning suggests that CJEU case law can be taken into account when interpreting provisions of the POPIA, whose drafting was based on the European data protection law.

In *Competition Commission of South Africa v Media 24 (Pty) Limited*,[40] on the other hand, Theron J rejected the adoption of CJEU case law in the context of section 8(c) of the Competition Act.[41] This judgment is of particular interest as Theron J argued for a limitation when taking foreign law into account while interpreting South African laws. The judge emphasised that foreign law can be considered for the interpretation of section 8(c) of the Competition Act but "should not displace the express meaning of the [South African] legislation".[42] Transferring this reasoning into the context of the POPIA, the adoption of CJEU case law would be out of question if such reference would displace the express meaning and systematisation of particular provisions or concepts as introduced by the Act.

35 (2015) ZACC 13 par 50, 75 ff.
36 (2017) 38 ILJ 295 (CC) 333 ff par 141 ff.
37 66 of 1995.
38 the *Horn* case (n 35) par 67; the *Rural Maintenance* case (n 36) 333 par 141.
39 In both minority judgments, Zondo J refers to the Council Directive 77/187/EEC (of 14 February 1977 on the approximation of the laws of the member states relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of businesses, OJ L 61, 5.3.1977, 26 ff) as well as the "1981 TUPE-Regulations", which transposed the directive into domestic UK law.
40 *Competition Commission of South Africa v Media 24 (Pty) Limited* 2019 5 SA 598 (CC) 631 ff par 98 ff, 655 par 185.
41 Act 89 of 1998.
42 the *Competition Commission* case (n 40) 655 par 185 (additions by the authors).

3 Specification of selected concepts of the Protection of Personal Information Act

The subsequent discussion will examine the CJEU case law in respect of three fundamental concepts of EU data protection law, which are also contained in the regulatory framework of the POPIA. This refers to the concepts of personal information, joint responsibility and consent.

3.1 The concept of "personal information"

Personal information is the key concept to determine whether the POPIA applies. It is, therefore, imperative to clarify the concept of "personal information" to determine the scope and application of the Act. Evaluating whether "personal information" is processed can be complex. For example, regarding the pandemic-related increased use of cloud services, an assessment needs to be conducted in respect of any information uploaded to the "cloud" to determine whether this information is classified as personal information. The same applies to pandemic-related measures such as COVID-19 tracing apps and the capturing of other information, like the personal details of restaurant patrons or individuals' vaccination statuses. Even though the pandemic has led to new forms of data processing, it should be noted that the gravity of the concept of "personal information" goes far beyond such pandemic related matters. This concept is the starting point of every data protection assessment and its practical relevance cannot be overemphasised.

After a brief overview of the concept of personal information under the POPIA, the paper will ascertain whether the adoption of the CJEU's reasoning in the case of *Breyer v Bundesrepublik Deutschland* could mitigate legal uncertainty in the new South African data protection framework.[43]

3.1.1 The definition of personal information

Section 1 of the POPIA generally defines personal information as "information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person". Along with this definition, the act provides a non-exhaustive list[44] of examples for personal information. The POPIA essentially adopted the

43 See Baumann and Ismail (n 1) 732 ff for a detailed discussion of the adoption of this judgment under the POPIA.

44 See Abdulrauf "Data protection in the internet: South Africa" in Moura Vincente and de Vasconcelos Casimiro (eds) *Data Protection in the Internet* (2020) 349 352; Burns and Burger-Smidt (n 29) 22 and Roos (n 25) 204.

concept of "personal data"[45] as provided for in international[46] and EU data protection laws.[47]

The most problematic requirement for information to be classified as "personal information" or "personal data" lies in determining whether it relates to an "identifiable person". Despite the history of more than 25 years of EU data protection, the criteria under which a person is "identifiable" remains a subject of controversial academic discussions. Thus far, it is still discussed to which extent third-party knowledge must be taken into consideration. Unlike the UK Data Protection Act 1998,[48] for example, neither the EU data protection law nor the POPIA explicitly address which entities knowledge is relevant to determine the identifiability of a person. In light of this, it appears to be fruitful to analyse the *ratio decidendi* of *Breyer v Bundesrepublik Deutschland*, which explicitly addressed this aspect.

3.1.2 The Breyer v Bundesrepublik Deutschland *case*

The CJEU interpreted the term "identifiable person" in the context of article 2(a) of the DPD in the 2016 judgment of *Breyer v Bundesrepublik Deutschland*.

The case dealt with the storing of information on all access operations in log files related to public websites of German Federal Institutions. The log files included, *inter alia,* the dynamic IP-Address of computers seeking access to prevent attacks on those websites and to enable the identification of attackers for criminal prosecution.

The *Bundesgerichtshof* requested a preliminary ruling to determine, *inter alia*, whether dynamic IP-Addresses are classified as personal data in terms of article 2(a) DPD for the website the provider

45 It should be noted that the South African and European concepts are not completely identical. *e.g.* regarding the protection of information relating to juristic persons. The POPIA follows a more extensive approach (*cf* Baumann and Ismail (n 1) 730 f and Roos "The European Union's General Data Protection Regulation (regulation) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles'" 2020 (3) *CILSA* 1 9 f).

46 See s 1(b) of the OECD Guidelines 1980 and s 2(a) of the Convention of the Council of Europe 1981.

47 See a 4(1) of the GDPR and the preceding definition of a 2(a) of the DPD.

48 See the definition of "personal data" under s 1 of the UK Data Protection Act 1998 which provides that '"personal data' means data which relate to a living individual who can be identified—(b) *from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller* [...]" (emphasis by the authors).

if a third party, such as an internet service provider, has the additional knowledge required to identify the data subject.[49]

As a starting point in addressing this question, the CJEU referred to recital (26) of the DPD.[50] This recital provided that when determining if a person is "identifiable", all means likely to be used, either by the controller or by any other person, to identify the said person should be taken into account. On this basis, the CJEU came to the conclusion that "it is not required that all the information enabling the identification of the data subject must be in the hands of one person".[51] Thereafter, the court held that "it must be determined whether the possibility to combine a dynamic IP address with the additional data held by the internet service provider constitutes a means likely reasonably to be used to identify the data subject".[52] The court then elaborated that those requirements are not met in cases where identification is legally prohibited or practically impossible.[53] According to the ruling, such a practical impossibility can be assumed when a disproportionate effort in terms of time, cost and man-power is required and the risk of identification appears to be insignificant in reality.[54] In respect of dynamic IP-Addresses, the court then reached the conclusion that the existence of legal means to obtain the information from the third party, such as an internet service provider, constitutes means that may reasonably be used to identify the data subject.[55]

3.1.3 The adoption of Breyer v Bundesrepublik Deutschland *under the Protection of Personal Information Act and alternative approaches*

From a South African perspective, the question remains whether an adoption of the *Breyer* decision is desirable and methodologically possible. German scholars, in particular, already discussed several distinctive approaches to ascertain the extent of third-party knowledge which should to be taken into account when determining whether a person is "identifiable" under the *Bundesdatenschutzgesetz*, which transposed the DPD into domestic law.[56] Out of the broad

49 OJ C 89, 16.3.2015, 4 f.
50 CJEU, *Breyer* case C-582/14 (2016) par 42.
51 CJEU, *Breyer* (n 50) par 43.
52 CJEU, *Breyer* (n 49) par 45.
53 CJEU, *Breyer* (n 49) par 46.
54 CJEU, *Breyer* (n 49) par 46.
55 CJEU, *Breyer* (n 49) par 47 f.
56 On the numerous approaches in this context, see Bergt "Die Bestimmbarkeit als Grundproblem des Datenschutzrechts—Überblick über den Theorienstreit und Lösungsvorschlag" 2015 *Zeitschrift für*

spectrum of approaches developed within the German discussion, two approaches to interpret the criteria of "identifiable" were widely supported and could be possible alternatives to interpret the concept of personal information under the POPIA. For this reason, the so-called "objective" or "absolute" approach, as well as the so-called "subjective" or "relative" approach will subsequently be examined as potential alternatives to the adoption of the CJEU's approach in the *Breyer* judgment.

3.1.3.1 The "objective" or "absolute" approach

The most extensive approach is the so-called "objective" or "absolute" approach. It classifies information as personal data when anybody is able to identify the person.[57] According to this approach, the entire world's knowledge would have to be taken into account.[58] The adoption of this approach under the POPIA would subject almost every processing of information to the Act, thereby contravening the purpose of this legislation to only regulate the processing of "personal" information.[59] In addition, the definition of the term "unique identifier" in section 1 of the POPIA[60] suggests that the perspective of the responsible party is of primary relevance. For those reasons, the objective approach should not be supported under the POPIA.

Datenschutz (ZD) 365 ff and Haase *Datenschutzrechtliche Fragen des Personenbezugs* (2015) 259 ff.

57 Pahlen-Brandt "Datenschutz braucht scharfe Instrumente Beitrag zur Diskussion um 'personenbezogene Daten'" 2008 *Datenschutz und Datensicherheit (DuD)* 34 38. For an absolute approach under the GDPR Buchner "Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO" 2016 *DuD* 155 156 and Weichert "DSGVO Art 4" in Däubler, Wedde, Weichert and Sommer *EU-DS-GVO und BDSG Kompaktkommentar* (2020) par 19 who acknowledges restrictions by recital (26) of the regulation.

58 See the remarks of the *Landgericht Berlin* 2013 *ZD* 618 619 where the objective approach was rejected in the result.

59 See s 2(b) of the POPIA. On this aspect see also Baumann and Ismail (n 1) 736 f.

60 The section reads as follows: "'unique identifier' means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely *identifies that data subject in relation to that responsible party*" (emphasis added).

3.1.3.2 The "subjective" or "relative" approach

The so-called "subjective" or "relative" approach is more restrictive and requires the controller to be able to identify the person concerned with reasonable effort.[61] The provisions of the POPIA also do not expressly support nor reject the subjective approaches, raising the question of whether it might be beneficial to follow this interpretation. The adoption of the subjective approach as supported in the UK Data Protection Act 1998 may be considered for the interpretation of the POPIA. In this regard, it needs to be noted that section 1 of the UK Data Protection Act 1998 was amended by section 3(2) of the UK Data Protection Act 2018[62] which does not support the subjective approach any longer. This approach would, therefore, result in the adoption of an already revised legal position.[63]

3.1.3.3 The adoption of the CJEU's approach in the Breyer case

The third option would, therefore, be the adoption of the approach as supported in the *Breyer* case. From the reasoning of the court in this judgment, scholars concluded that the CJEU does not follow the objective approach,[64] but supports a moderate subjective approach which includes elements of the objective approach.[65] This approach takes into account the means and additional knowledge that the controller will reasonably use for identification.[66] Under the GDPR,

---

61 *e.g. Landgericht Frankenthal* 2008 *Multimedia und Recht (MMR)* 687 689; Eckhardt "IP-Adresse als personenbezogenes Datum – neues Öl ins Feuer" 2011 *Computer und Recht (CR)* 339 342; Roßnagel and Scholz "Datenschutz durch Anonymität und Pseudonymität" 2000 *MMR* 721 723. Also see s 1 of the UK Data Protection Act 1998 (n 47). In context of the GDPR Hofmann and Johannes "DS-GVO: Anleitung zur autonomen Auslegung des Personenbezug" 2017 *ZD* 221 226 and Selzer in Jandt and Steidle (eds) *Datenschutz im Internet* (2018) 128.

62 This section reads as follows: "'Personal data' means any information relating to an identified or identifiable living individual …".

63 Baumann and Ismail (n 1) 737.

64 Moos "Anmerkung zu EuGH, Urteil vom 19.10.2016–C-582/14–Breyer" 2016 *MMR* 845.

65 Karg "Art 4 Nr 1 DSGVO" in Simitis, Hornung and Spiecker gen Döhmann (eds) *Datenschutzrecht* (2019) par 60; Mantz and Spittka "Anmerkung zu EuGH (2 Kammer), Urteil vom 19.10.2016–C-582/14 (Breyer/ Deutschland)" 2016 *Neue Juristische Wochenschrift (NJW)* 3582 3583; Moos (n 64) 845.

66 Article 29 of the Data Protection Working Party *Opinion 4/2007 on the concept of personal data WP 136* (20.6.2007) 15; Brink and Eckhardt "Wann ist ein Datum ein personenbezogenes Datum?" 2015 *ZD* 205 210 f.

the majority supports this moderate approach[67] with reference to recital (26) of the Regulation[68] and the leading CJEU case of *Breyer*.[69]

Several arguments can be invoked in support of the adoption of this approach under the POPIA.[70] The *Breyer* judgment is the leading case in the interpretation of an "identifiable person" in all EU member states. Thus, an adoption of the CJEU's reasoning would support the aim of the POPIA to regulate the processing of personal information in harmony with international standards.[71] The similarity of the wording of the definition of personal information under the POPIA and the definitions in European data protection law strongly indicate that the CJEU's interpretation would not displace the express meaning of "personal information" under the POPIA. The genesis and systematic interpretation of the Act support this position. Firstly, the historical connection between the POPIA and the DPD[72] provide a basis to adopt the EU case law. Secondly, the provisions of the POPIA can be interpreted in favour of the moderate subjective approach. While the definition of "unique identifier" indicates a perspective centred to the responsible party, the definitions of "re-identify" and "de-identify"[73] refer to "reasonably foreseeable" methods to identify the data subject or to link data by such a method that identifies the data subject. This

67 *e.g.* Gola "Art 4 DS-GVO" in Gola (ed) *Datenschutz-Grundverordnung VO (EG) 2016/679 Kommentar* (2018) par 18; Schantz in Schantz and Wolff *Das Neue Datenschutzrecht* (2017) par 279; Schreiber "Artikel 4 DSGVO" in Plath *DS-GVO/BDSG* (2018) par 8; Karg (n 65) par 61 ff; Rücker "B. Scope of application of the regulation" in Rücker and Kugler (eds) *New European General Data Protection Regulation* (2018) par 91 (referring to recital (26) of the regulation).

68 Recital (26) s 3 and 4 of the GDPR read as follows: "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments".

69 See above 3.1.2.

70 See also the arguments provided by Baumann and Ismail (n 1) 737 ff.

71 See s 2 of the POPIA.

72 The definition of "personal data" in terms of the DPD formed the starting point of the discussion in the proceedings of the SALRC (*Issue Paper 24 (Project 124)* (2003) sub. 2.48). During those proceedings, the commission then opted to utilise the term "personal information" (SALRC, *Project 124 Privacy and Data Protection Report* (2009), sub 3.1.6).

73 See s 1 of the POPIA.

"reasonability test" applies in the context of section 6(1)(*b*) of the POPIA which determines whether the application of the Act is excluded. In light of this, the sole reference to the perspective of the responsible party appears to be too restrictive and would render the "reasonability test" meaningless in cases where the responsible party can access the relevant information or apply means to identify the data subject with reasonable efforts.

3.1.3.4 Interim conclusion

In the light of the aforementioned, the adoption of the CJEU's reasoning in the *Breyer* judgment appears desirable as it provides guidance on how to determine whether a person is "identifiable" in terms of section 1 of the POPIA. Furthermore, reference to this case law would also be in accordance with the methodical requirements as deduced from the Constitutional Court's recent decisions where case law of the CJEU was considered when interpreting South African legislation.[74]

3.2 The concept of joint responsibility

Under the POPIA, the concept of joint responsibility is closely connected to the principle of accountability as set out in section 8 of the Act which provides that the "responsible party" must comply with the provisions of the Act. Section 1 of the POPIA defines the responsible party as "a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information". From a South African perspective, this definition may be regarded as just another "black box" of the new act, as its highly abstract formulation seems difficult to apply in practice. This concerns cases of joint responsibility whereby an entity determines the purpose and means of processing "in conjunction" with other entities. Therefore, a potential joint responsibility needs to be considered as soon as two entities collaborate and administer a particular processing of personal information. For example, this applies to the highly relevant commercial use of social media, which advanced as an important business tool for many small and midsize businesses (SMB) during the pandemic.[75]

74 In detail above 2.2.

75 According to a Genesis Analytics study (commissioned by Facebook), 65% of the surveyed SMB's increased their use of social media during the pandemic (Genesis, *How social media is powering small businesses in Africa* (2021) 8 (https://www.genesis-analytics.com/reports-and-other-

In the European data protection framework, the concept of (joint) controllership has been established in 1995 by article 2(d) of the DPD.[76] Under the GDPR, this definition was retained[77] and flanked by the newly introduced article 26, specifically regulating the consequences of joint controllership. The basis of controllership is the authority to determine the purposes and means of processing, therefore, the fact that data are actually processed is not decisive.[78] The identification of facts that constitute joint controllership, on the other hand, has proven to be complex. In three decisions, the CJEU interpreted and specified the concept of joint controllership.[79] After introducing these landmark judgments, a possible reception of this case law under the POPIA will be examined, taking into account whether it meets the requirements as set out by the Constitutional Court.

3.2.1 The CJEU on joint controllership—three landmark decisions

In the three landmark decisions on joint controllership under the DPD, the CJEU started a process to clarify this nebulous legal concept. Those decisions will subsequently be discussed and criteria to allocate joint controllership will be deduced from the CJEU's reasoning.

3.2.1.1 *ULD Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein*

In *ULD Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein*, the CJEU dealt with the question of whether the operator of a *Facebook* fanpage is jointly responsible with the social network, *Facebook,* for data processing.

The court stated that the mere use of a social network does not establish joint responsibility for the data processing carried out by the network.[80] The CJEU also pointed out that the operator of a fanpage enables the possibility for the social network to place cookies on devices of persons who visit this fanpage, regardless

documents/how-social-media-is-powering-small-business-in-africa-report (08-01-2022)).

76 The provision reads as follows: "'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data…".

77 See a 4(7) of the GDPR.

78 CJEU, the *FashionID* case C-40/17 (2019) par 82.

79 CJEU, the *Wirtschaftsakademie* case C-210/16 (2018); CJEU, the *Jehovan* case C-25/17 (2018); CJEU, *FashionID* (n 78).

80 CJEU, *Wirtschaftsakademie* (n 79) par 35.

of whether they are users of the social network or not.[81] The court held that the responsibility of the fanpage operator, regarding the processing of personal data of persons who are not users of the social network, should be regarded as "even greater" since accessing the fanpage automatically triggers such processing.[82] The possibility of controlling or promoting the data processing by the fanpage operator was considered as relevant participation in the determination of the purposes and means of processing.[83] In this case, the fanpage operator could define parameters on its target audience in order for the social network provider to generate user statistics.[84] Moreover, the court held that joint controllership does not require each entity involved to have access to the personal data concerned.[85]

3.2.1.2 The *Jehovan todistajat*-case

In the *Jehovan todistajat* case, the CJEU discussed joint controllership between the religious community of Jehovah's Witnesses and its members who engage in the processing of personal data when preaching door-to-door.[86]

In this decision, the court emphasised that an influence on the data processing out of self-interest and the accompanying joint decision on the purposes and means of the processing would establish joint controllership.[87] The court reiterated that joint responsibility does not require all parties involved in data processing operations to have access to the personal data concerned.[88] Conclusively, the CJEU affirmed joint controllership of the religious community because it organises, encourages and co-ordinates the processing of personal data by its members.[89]

3.2.1.3 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*

In the *FashionID* case, the CJEU ruled on the joint controllership between a website operator who embedded a social plugin (the

81 CJEU, *Wirtschaftsakademie* (n 79) par 35.
82 CJEU, *Wirtschaftsakademie* (n 79) par 41.
83 CJEU, *Wirtschaftsakademie* (n 79) par 36, 39.
84 CJEU, *Wirtschaftsakademie* (n 79) par 36.
85 CJEU, *Wirtschaftsakademie* (n 79) par 38.
86 CJEU, *Jehovan* (n 79) par 63 ff.
87 CJEU, *Jehovan* (n 79) par 68.
88 CJEU, *Jehovan* (n 79) par 69.
89 CJEU, *Jehovan* (n 79) par 72 f.

Facebook "Like" button) into his website and the provider of this plugin (in this case, the social network *Facebook*).[90]

In this judgment, the court emphasised that an influence on the processing and the accompanying joint decision on the purposes and means can establish joint controllership.[91] The court restated that joint responsibility does not require that all parties have access to the personal data in question.[92] Thereafter, the CJEU held that the integration of the "Like" button into the *FashionID* website enabled *Facebook* to obtain personal data of the website visitors, whether they were members of the social network or not.[93] The ruling qualifies this as a joint decision on the means and purposes of the processing.[94] With regard to the means of processing, the court emphasised that *FashionID* included the "Like" button with the knowledge that it served as a tool for collecting and transmitting data from website visitors, which "exerts a decisive influence" over *Facebook's* data processing.[95] Further, the ruling identified that both *FashionID* and *Facebook* would acquire economic interests regarding the data processing carried out.[96] The court also pointed out that *FashionID's* responsibility appears to be "even greater" regarding the processing of personal data of website users that are not users of the social network *Facebook*, since accessing the website automatically triggers data processing by *Facebook*.[97]

3.2.1.4 Criteria for the allocation of joint controllership

The discussion of these landmark decisions on the concept of joint controllership illustrates that the CJEU's reasoning strongly focussed on the underlying facts of the cases. Nevertheless, the Court introduced some general principles. Firstly, it was clarified in all judgments that joint controllership does not require that all parties have access to the personal data in question.[98] This denotes that factual access or control over the data is not the decisive criteria for controllership. Secondly, the court repeatedly stated that a joint responsibility does not necessarily imply equal responsibility for the various entities

90 CJEU, *FashionID* (n 78) par 64 ff.
91 CJEU, *FashionID* (n 78) par 68.
92 CJEU, *FashionID* (n 78) par 69.
93 CJEU, *FashionID* (n 78) par 75.
94 CJEU, *FashionID* (n 78) par 76.
95 CJEU, *FashionID* (n 78) par 77 f.
96 CJEU, *FashionID* (n 78) par 80.
97 CJEU, *FashionID* (n 78) par 83.
98 CJEU, *Wirtschaftsakademie* (n 79) par 38; CJEU, *Jehovan* (n 79) par 69; CJEU, *FashionID* (n 78) par 69.

involved in the processing of personal data.[99] This introduces the possibility of a flexible allocation regarding the legal consequences of joint controllership among the respective entities.

Furthermore, abstract criteria for the allocation of joint controllership can be deduced from the abovementioned landmark decisions. From the *Wirtschaftsakademie* judgment, it can be deduced that the influence of an entity to steer the particular purposes of data processing is sufficient to assume joint controllership.[100] From the *Jehovan todistajat* judgment, it can be inferred that encouraging and facilitating, through organisation and coordination, of other entities' processing activities can be regarded as a basis for joint controllership.[101] In the *FashionID* judgment, the CJEU clarified that an economic interest of the involved entities is a relevant factor in the allocation of joint controllership.[102] On the basis of these criteria, it is possible to derive guidelines for the allocation of joint controllership in other cases where several entities are involved in the processing of personal information.

3.2.2 Adopting the flexible concept of joint controllership under the POPIA

A reception of the CJEU's landmark judgments could be beneficial under the South African data protection framework as it would mitigate legal uncertainty in determining the (jointly) responsible parties. This would also apply in pandemic-related processing of personal information, such as the operation of the COVID-19 tracing app or the recent spike in the use of social media networks. It could also provide a flexible instrument to *pro futuro* identify responsible parties regarding emerging technologies within the transformation of the Fourth Industrial Revolution, where personal information is processed involving several entities (for example in blockchain-networks).[103]

In adopting the CJEU case law, South African courts and supervisory authorities could promote joint responsibility to an instrument that, due to its flexibility and the low requirements for

99 CJEU, *Wirtschaftsakademie* (n 79) par 43; CJEU, *Jehovan* (n 79) par 66; CJEU, *FashionID* (n 78) par 70.

100 See above 3.2.1.1.

101 See above 3.2.1.2.

102 See above 3.2.1.3.

103 ***Cf*** Baumann and Hamm "Datenschutzrechtliche Verantwortlichkeit in privaten Blockchains" in Taeger (ed) *Im Fokus der Rechtsentwicklung—Die Digitalisierung der Welt* (2021) 221 226 ff, on the allocation of joint controllership in private Blockchain networks.

the assumption of joint responsibility, bears the potential to increase the protection of personal information through a broader distribution of accountability. From a methodical perspective, the genesis of the POPIA[104] as well as the similarity of the definition of "responsible party" as provided by the act strongly indicate that reference to the discussed CJEU case law would not displace the meaning of the concept of joint responsibility under the POPIA. Scholars have already emphasised that the POPIA's definition is almost identical to the definition in the European framework.[105]

3.3 The concept of consent

Any processing of personal information regulated by the POPIA must be lawful, which requires a ground for processing as stipulated in section 11(1) of the Act. Those general grounds for lawful processing are very similar to the grounds of processing[106] within the European data protection law.[107] It is, therefore, not a coincidence that the POPIA also recognises consent as a ground for processing.[108]

Consent is an ambivalent basis for the processing of personal information. On the one hand, it can justify the processing of personal information based on an informed and free decision of the data subject, even when other grounds for processing are inapplicable. On the other hand, the requirements for valid consent are relatively strict and the data subject may withdraw consent at any given time.

The POPIA defines consent as "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information".[109] The similarity of this definition to the definition of article 2(h) of the DPD is apparent.[110] Under the GDPR, an even more detailed definition of consent was introduced[111] along with special provisions specifying the requirements

104 See above 2.1.
105 Roos (n 45) 11.
106 See a 7 of the DPD and a 6(1) of the GDPR.
107 *Cf* Baumann and Ismail (n 1) 721 and Roos (n 45) 17 ("grounds are similar").
108 See s 11(1)(*a*) of the POPIA.
109 See s 1 of the POPIA.
110 The definition of a 2(h) read as follows: "'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".
111 See a 4(11) of the GDPR, defining consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by

of consent.[112] The POPIA also provides further provisions related to the concept of consent in section 11(2), addressing the burden of proof which is placed on the responsible party and the right to withdraw consent at any time, clarifying that the withdrawal only eliminates the legal basis to process personal information *ex-nunc*.

The standing of "consent" within the grounds of processing[113] and the interpretation of the requirements for valid consent in data protection law are directly correlated to the extent to which a data protection regime attaches legitimising effects to the decision of the data subject, thereby potentially endorsing informational self-determination.[114] In two recent decisions, that will subsequently be discussed, the CJEU strengthened the autonomy of the data subject when consenting to data processing via so-called opt-out settings by introducing the requirement of active consent. Opt-out settings

---

which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

112 See a 7 and 8 of the GDPR.

113 Under the GDPR, some scholars opine that consent should take precedence over other grounds of processing (see *e.g.* Frenzel "DS-GVO Art. 6" in Paal and Pauly (eds) *DS-GVO BDSG* (2018) par 10). Other scholars argue for a subsequent application of consent *de lege ferenda* (Radlanski *Das Konzept der Einwilligung in der datenschutzrechtlichen Realität* (2016) 206 ff; Voigt *Die datenschutzrechtliche Einwilligung* (2020) 475 ff). *De lege lata*, the majority of scholars support the opinion that the grounds of processing of a 6(1) of the GDPR are independent and of an equal rank (*e.g.* Funke *Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht* (2017) 112; Kelleher and Murray *EU Data Protection Law* (2018) par 7.02; Kotschy "Art 6" in Kuner, Bygrave and Docksey (eds) *The EU General Data Protection Regulation A Commentary* (2020) sub C 1.1; Krusche "Kumulation von Rechtsgrundlagen zur Datenverarbeitung" 2020 *ZD* 232 233).

114 The German *Bundesverfassungsgericht* deduced a fundamental right of informational self-determination from a 1(1) and 2(1) of the *Grundgesetz* (*Bundesgesetzblatt* I (1949) 1 ff) in its 1983 landmark decision, the so-called *Volkszählungsurteil*. This right includes the right of the individual "to decide for himself when and within what limits personal matters are to be disclosed" (BVerfGE 65, 1, 42 (translated by the authors)). A number of scholars support a similar interpretation of the fundamental right to protection of personal data as provided by a 8 of the Charter of Fundamental Rights of the European Union (OJ C 326, 26.10.2012, 391 ff), see de Terwangne *The Right to be Forgotten and the Informational Autonomy in the Digital Environment* (2013) 5; Lynskey "Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order" 63 *ICLQ* (2014) 569, 591 f; such an interpretation is rejected by Kranenborg in Peers, Hervey, Kenner and Ward (eds) *The EU Charter of Fundamental Rights: A Commentary* (2014) Part I par 08.25 f.

typically place the burden of action to refuse consent on the data subject.[115] In opt-in settings, the data subject is typically required to consciously exercise control and decide whether to consent.[116] Practically, the design of the consent procedure is of significant relevance, as consumers tend to choose the option that has been marked as a default, leading to a higher likelihood for consent in an opt-out default setting.[117]

During the pandemic, people became more aware of the legal implications of consent. Many activities that forms part of the pandemic's everyday life requires individuals' consent, for example, COVID-19-testing, vaccinations or the disclosure of a person's vaccination status. In addition, consent of the data subject is also requested when using the Covid Alert SA app[118] and numerous web-services. In light of the pandemic driven spike in the number of users of such web-services, the concept of consent is of high practical relevance for the legitimate processing of personal information. The idea of adopting the concept of active consent should be explored due to the imminent potential to strengthen data subjects' autonomy.

3.3.1 The inception of "active" consent by the CJEU

The concept of active consent was firstly introduced in the CJEU's 2019 *Planet49* judgment, where the court interpreted the definitions of consent under the DPD and the GDPR. In the 2020 *Orange România* case, the court confirmed the concept of active consent and discussed aspects related to the burden of proof.

3.3.1.1 *Verbraucherzentrale Bundesverband eV v Planet49 GmBH*

The decision of the CJEU in *Planet49* is based on a request for a preliminary ruling by the *Bundesgerichtshof*.[119] The *Bundesgerichtshof* was confronted with the question of whether consent to the use of cookies in the context of a "free" online competition by means of a

115 For greater detail on different opt-out designs see Krohm "Abschied vom Schriftformgebot der Einwilligung—Lösungsvorschläge und künftige Anforderungen" 2016 *ZD* 368, 372 f.

116 Van Oijen and Vrabec "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective" 42 *Journal of Consumer Policy* (2019) 91 99.

117 In greater detail *cf* Van Oijen and Vrabec (n 116) 98 f.

118 The users of this app are required to consent to the processing of personal information as indicated in the privacy policy (*cf* https://sacoronavirus.co.za/covidalert/privacy-policy/ (08-01-2022)).

119 OJ C 112, 26.3.2018, 9 f.

preselected checkbox (so-called opt-out setting) is valid. The question referred to the Court was whether valid consent was given in terms of article 5(3) and article 2(f) of the ePrivacy-Directive[120] in conjunction with article 2(h) of the DPD and article 6(1) of the GDPR.

Regarding the concept of consent in terms of article 2(h) of the DPD, the CJEU ruled that "the requirement of an 'indication' of the data subject's wishes clearly points to active, rather than passive, behaviour".[121] According to the Court, consent given by way of a preselected tick in a checkbox does not imply active behaviour by the user of a website.[122] The Court also stated that this interpretation is supported by the requirement that the data subject's consent must be given "unambiguously", as provided for in article 7(a) of the DPD.[123] In addition, the court referred to the revision of article 5(3) of the ePrivacy directive in 2009, when the wording of this provision was substantially amended from the requirement that the user had the "right to refuse" the storage of cookies which was amended to "given his or her consent". The CJEU deduced from this legislative development that users' consent may no longer be presumed and must be the result of active behaviour.[124]

Thereafter, the Court noted that the wording of article 4(11) of the GDPR "appears even more stringent" than that of its predecessor article 2(h) of the DPD.[125] With reference to recital (32) of the regulation,[126] the CJEU concluded that the concept of active consent is explicitly recognised under the GDPR.[127] In this context, the CJEU

120 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, 37 ff.

121 CJEU, *Planet49* (n 18) par 52.

122 CJEU, *Planet49* (n 18) par 52.

123 CJEU, *Planet49* (n 18) par 54.

124 CJEU, *Planet49* (n 18) par 56.

125 CJEU, *Planet49* (n 18) par 61.

126 The recital reads as follows: "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent…".

127 CJEU, *Planet49* (n 18) par 62.

specifies that the recital "expressly precludes 'silence, pre-ticked boxes or inactivity' from constituting consent".[128]

3.3.1.2 *Orange România SA v ANSPDCP*

In *Orange România*, the CJEU dealt with the question of proof regarding valid consent upon a preliminary ruling request by the *Tribunalul București*.[129] *Orange România,* a telecommunication service provider, allegedly collected and stored copies of customers' identity documents without their consent. *Orange România* requested customers to consent to the retention of copies of their identity documents when concluding mobile phone contracts. The relevant checkbox, including the consent clause, was ticked by *Orange România's* sales staff before the actual contract was handed over to the customer for signature.[130] In the event of refusal of this consent, the company's practice required the customer to sign an additional form expressing the refusal of consent.[131] As a result, the Romanian data protection authority, *ANSPDCP,* imposed a fine and ordered *Orange România* to destroy the copies of customers' identity documents. The order was subsequently challenged in court.

In the ruling, the CJEU confirmed the normative basis for the requirement of active consent.[132] Thereafter, the court stated that pursuant to article 7(1) of the GDPR, the controller bears the burden of proof for valid consent and must be able to demonstrate that the data subject has consented to the respective processing.[133] The mere fact that the box was ticked, in the light of the evidence that the consent clauses had been ticked by sales staff, was considered to be insufficient to prove a positive indication of consent by the customers.[134] In addition, the fact that the customers signed the contracts, including the ticked consent clause, was also considered insufficient to prove valid consent as there was no evidence that this clause had actually been read and understood by the customers.[135]

3.3.2 Adopting "active" consent under the POPIA

Taking into account the similar wording of the definitions of consent under the POPIA and the DPD, an adoption by South African courts of

128 CJEU, *Planet49* (n 18) par 62.
129 The request is accessible via https://bit.ly/3yun7Jm (08-01-2022).
130 CJEU, the *Orange România* case C-61/19 (2020) par 45.
131 CJEU, *Orange România* (n 130) par 45.
132 CJEU, *Orange România* (n 130) par 35–37.
133 CJEU, *Orange România* (n 130) par 42.
134 CJEU, *Orange România* (n 130) par 46.
135 CJEU, *Orange România* (n 130) par 46.

the concept of active consent with reference to the *Planet49* case would be in line with the methodical requirements as indicated by the judges of the Constitutional Court.[136] Nevertheless, the introduction of active consent into South African data protection law would create significant implications and requires careful consideration. The question of whether an opt-in or opt-out consent should be supported under the new South African data protection framework was extensively discussed during the legislative process.[137] The remarks in the 2009 SALRC Report favoured an opt-out consent approach and indicated that consent could be inferred from "(in)action".[138]

This position, which indicates that valid consent does not require active behaviour, has not been incorporated explicitly in the definition of consent under the POPIA, it was merely articulated in the SALRC report. An adoption of the *Planet49* judgment would, therefore, technically not displace the meaning of the POPIA. The South African courts could use the term "expression" within the definition of consent in section 1 of the POPIA as an anchor to introduce the requirement of active behaviour of the data subject.[139] Such an interpretation could strengthen the informational self-determination of data subjects significantly. In the 2005 SALRC discussion paper, the commission itself highlighted the role of privacy as one of the core democratic values emphasising that the preservation of privacy fosters, *inter alia*, self-determination.[140] This could provide an additional argument in favour of active consent.

On the other hand, the courts would have to bear in mind that a higher degree of self-determination also increases the data subject's responsibility. A recognition of active consent would result in an increase of situations where the data subject will have to decide whether it wants to consent to a particular processing of personal

136 In detail above 2.2.

137 SALRC *Discussion Paper 109 (Project 124)* (October 2005) sub 4.2.43 ff.

138 See SALRC *Project 124 Privacy and Data Protection Report* (2009) sub 4.2.63: "Thus, for instance, if a person was informed of an intention on the part of the responsible party to use his (non-sensitive) information for a specific purpose, and was offered the opportunity to object to this use (e.g., by means of a negative tick-box on a form), yet did not use this opportunity (ie by returning the form without the box being ticked), his consent to the use of his information can be inferred from this (in) action".

139 *Cf* the similar reasoning of CJEU regarding the term "indication" under a 2(h) DPD in CJEU, *Planet49* (n 18) par 52.

140 See SALRC, *Discussion Paper 109 (Project 124)* (October 2005) sub 2.1.1 with footnote 2.

information and actively declare its consent (for example, via opt-in). In this regard, scholars emphasised that this could result in a "consent overload"[141] or a "consent fatigue"[142] whereby the data subject does not perceive their decision to consent to be a meaningful decision.

Regarding the evidentiary burden of the concept of active consent, the South African courts would not have to adopt the CJEU's reasoning in the *Orange România* decision as section 11(2)(*a*) of the POPIA explicitly allocates the burden of proof for the data subject's consent to the responsible party. Should the South African courts interpret the definition of consent under the POPIA in favour of active consent, the burden of proof for the responsible party in terms of section 11(2)(*a*) of the POPIA would include the requirement of active behaviour of the data subject as the provision refers to "consent" in terms of section 1 of the POPIA.

4 Conclusion

The preceding paragraphs illustrate the potential to clarify the South African data protection framework under the POPIA through the adoption of the established case law of the CJEU. In times of a pandemic, this could be an opportunity to quickly mitigate legal uncertainty with reference to established case law, eliminating the need for a lengthy process of South African case law development.

The three key concepts discussed in this paper show a high similarity with the corresponding concepts in the European data protection framework, which provides a methodical basis to adopt the CJEU's case law. A case where the reception of the European case law would "displace the express meaning of [South African] legislation", as Theron J articulated, could not be identified. An endorsement for the adoption of the discussed landmark judgments by the Information Regulator or courts would provide clarity on how to interpret those key concepts of the POPIA, thereby promoting legal certainty. This applies to the concept of personal information, where an adoption of the *Breyer* judgment could clarify the interpretation and gravity of the Act's material scope. Regarding the concept of joint responsibility, abstract criteria to allocate controllership can be deduced from the three landmark decisions of the CJEU. This case law could be a

141 Engeler and Marosi "Planet49: Neues vom EuGH zu Cookies, Tracking und ePrivacy" 2019 *CR* 707 713.

142 Schermer, Custers and van der Hof "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection" 2014 *Ethics and Information Technology* 171 176 f.

starting point to shape the concept of joint responsibility under the POPIA. Lastly, the adoption of the *Planet49* judgment could provide a basis for the requirement of active consent under the POPIA. The requirement of active behaviour would strengthen the informational self-determination of data subjects and promote individual autonomy during the pandemic and thereafter.

Whether the South African courts and the Information Regulator will support an interpretation of the POPIA in light of the established EU case law *pro futuro* is unclear at this stage. From a methodical perspective, such an EU-infused interpretation of the investigated concepts appears to be possible. Insofar as the historical connection to the EU data protection law provides a basis for the adoption of CJEU case law in accordance with the Constitutional Court's considerations. Furthermore, this comparative approach bears the potential to mitigate the pressure on the POPIA to evolve by providing a solid basis in the long run and not only a "quick fix". From an economic point of view, the adoption of CJEU case law might also be advantageous. Should South African policymakers decide to advocate for an adequacy decision by the EU commission to enable free flow of data from the EU without requiring further authorisation,[143] which is a significant economic factor these days,[144] the commission will have to, *inter alia*, take into account the existence and effectiveness of data protection legislation and supervision as well as the case law in the third state.[145] In that case, the adoption of CJEU case law might be advantageous for South African enterprises and institutions.

143 See a 45(1) of the GDPR.

144 See for example the economic evaluation of the European Parliament concerning the data flow to the US European Parliament, *Resolution of 26 May 2016 on transatlantic data flows* (2016/2727(RSP)) (28.2.2018), OJ C 76/82 sub F and G.

145 See a 45(2)(a) and (b) of the GDPR.