IV. Fitting the Blockchain Solution into the GDPR Puzzle

This chapter assesses the proposal of leveraging blockchain technology for personal data protection by establishing a digital identity management platform on the touchstone of the GDPR. It is done by systematically mapping the compatibility of the proposal to the established principles of data protection as codified in the GDPR. However, this chapter begins with a general analysis of the GDPR's claim to technological neutrality.

A. GDPR: A Technolog(icall)y Neutral Law?

This part endeavours to evaluate the claim that the GDPR is a technologically neutral law.[101] Hilderbrandt and Tielmans give a lucid distinction between 'technology neutral law' and 'technologically neutral law'.[102] While 'technology neutral law' pertains to the understanding that legal effect should not depend on a particular technology used by those addressed by the law, use of the term 'technologically neutral law' is reserved to the notion that law does not depend on the articulation of a technology.[103] Hilderbrandt and Tielmans challenge this second approach by calling it a misconception. According to them, law can never be technologically neutral because it is always enabled by a particular technological ICT infrastructure.[104]Therefore, the assessment with regard to GDPR ought to be whether it is a 'technology neutral law'.

At the outset it is essential to understand the raison d'être of the GDPR. It is an established principle of law and economics that regulation is a response to externalities that impose a social cost.[105] Traditionally in the context of data protection, the externality appeared in form of imbalance of power between state and individual where the state wielded the upper

[101] Recital 15 GDPR.

[102] Mireille Hilderbrandt and Laura Tielmans, 'Data Protection by Design and Technology Neutral Law' (2013) 29 Computer Law and Security Review 509, 516.

[103] ibid.

[104] ibid.

[105] Ronald H Coase, 'The Problem of Social Cost' (1960) 3 Journal of Law and Economics 1.

hand in terms of collection, use and retention of data. However, over the years the rising economic potential of data has called for a re-evaluation of this approach to regulation and it makes a case for recognizing the private commercial interests in accumulating and processing data with the increasing technological ease. Therefore, the reform can be seen as a response to the technological externalities of advances in high-speed networking and data storage. The social cost imposed by these technological externalities was recognised by the Article 29 Data Protection Working Party Report, where it stresses the risk of lack of control and information asymmetry.[106]Information asymmetry is characterized by the significant gap between the data controller's and data subject's knowledge about the fate of the latter's personal data.[107]

Given that the GDPR is a response to technological externalities that threaten privacy and data protection, it is desirable to analyse the GDPR according to the three interpretations of technology neutral legislation propounded by Hilderbrandt and Tielmans. The three interpretations are as under:

1) In order to be neutral, law may have to provide for technology specific provisions to retain the substance of the legal right they support. The aim is to achieve equivalent effect in online and offline environments.
2) Legislation should not discriminate between different kinds of technologies with the same functionality because this could stifle innovation and result in unfair competition.
3) There is an underlying need for legislation to be future proof because legislative acts take a long time to reach fruition and the focus on a particular technology may render the legislation outdated and ineffective sooner than expected.[108] (emphasis added)

The GDPR, in all its technology neutral glory, still states data protection by design and default as one of its fundamental features.[109] Article 25 warrants for technical and organizational measures, in particular suggesting pseudonymisation, designed to implement data protection principles. In

[106] Article 29 Data Protection Working Party (2014) 'Opinion 8/2014 on the on Recent Developments on the Internet of Things', WP 223, 6.

[107] Janice Y Tsai et al, 'The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study' (2011) 22(2) Information Systems Research 254, 1.

[108] Hilderbradnt and Tielmans (n 102) 510.

[109] Article 25 GDPR.

this regard the technology specific nature of the provision, where technology itself is visualized as creating equivalent protection. Therefore, technological specificity embodied in Article 25 is needed to achieve technology neutral legislation. Secondly, parallel to data protection by design, the GDPR confers upon the data subjects a right to data portability, which has strong links to interoperability as a pre-requisite for dynamic efficiency.[110] This facilitates different technologies to thrive because it empowers the data subject to demand portability from one data controller to another, perhaps using different technology to ensure a more privacy friendly default. This achieves non-discrimination against technologies by the GDPR. Lastly, given the long and uncomfortable journey of the data protection law reform, the GDPR provisions are formulated in a manner so as to allow sufficient sustainability if not eternity of their relevance in a fast changing technological landscape.[111]

It flows from the above discussion that the GDPR has all the requisite features for being considered a technology neutral law. However, the mettle of this claim can be truly assessed only in light of a real confrontation. The blockchain model for digital identity management confronts the GDPR to prove its technology neutral credentials in practice.

It is the author's understanding that eventually the receptiveness of GDPR to revolutionary technologies like Blockchain would depend upon the kind of regulatory instrument the GDPR is categorised as.[112] Categorising it as a command and control regulatory instrument would mean that it is a 'classical' regulation operating through rule-based coercion. But if it were seen as falling within the class known as 'consensus', then it would be more likely to accommodate a digital identity management solution based on blockchain. The latter class of the regulatory instrument entails an exceptionally broad range of regulatory arrangements.[113] This ranges from 'self-regulation' to various forms of co-operative partnerships

[110] Article 20 GDPR.

[111] An example could be the phrasing of 'right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her' in Article 22 GDPR.

[112] For an understanding of different regulatory instruments. Brownen Morgan and Karen Yeung, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press 2007) Ch 3, 79.

[113] ibid 92.

between state and non-state actors in an attempt to regulate.[114] It has been claimed that industry self-regulation is more efficacious where the regulated activity (in this case being collection, storage and processing of personal data on a blockchain) is thought to require a high level of technical or expert knowledge, owing to superior informational capacities as compared to the state. Flexibility and adaptability to new technological needs are advantages of self-regulation over command and control regulation.

However, self-regulation has its limitations like absence of formal government approval and inadequacy of leniency to achieve public goals to mention a few. Hirsch highlights that in the absence of guarantees to legal compliance, a puritan form of self-regulation will ‘neither attract sufficient industry involvement nor address the need for international privacy standards’.[115] Therefore, what is desirable is something on the other side of the spectrum of possibilities offered by consensus kind of regulatory instruments –co-regulation. Standardisation can be one way of achieving co-regulation. The European Commission recently published its decision on a standardisation request towards the European Standardisation Organisations (ESOs).[116] This request is a Commission Implementing Decision based on the Regulation 182/2011.[117] This request entails a mandate, if accepted by the ESOs, for developing privacy management standards. In as much as it involves oversight by the Commission, this standard setting activity by the ESOs falls within the domain of co-regulation. Although the mandate pertains to the DPD, but since the GDPR itself recognises standardization and certification, it can be said that such standard setting activity would have a mandate under GDPR to co-regulate.[118] This creates a window for a blockchain based digital identity management platform to

[114] ibid.

[115] Dennis D Hirsch, ‘In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct’ (2013) 74 Ohio State Law Journal 1029, 1043.

[116] European Commission (2015) M/530 Commission Implementing Decision C(2015) 102 final of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy

[117] OJ L 55, 28/2/2011

[118] Articles 42,43 GDPR.

find compatibility with the GDPR if it can prove its credentials during the standard setting process at the ESOs. However, the standard setting process has to keep in mind that the participating technology is compliant with mandatory legal requirements.[119] This implies that if a blockchain based digital identity management solution can assert that it is compliant with the legal requirements of the GDPR and if it is able to prove its technological credentials, it may be incorporated as a technical standard for data protection by design. According to Falke et al, 'compliance with standards may create 'legitimate expectations' and people may assume them to have official legal standing'.[120] This will root the legal status of a blockchain-based solution by way of co-regulation.

The GDPR cannot weather the storm of emerging technologies solely by relying on the sufficiency of the new legal provisions. In so far as the mandate is seen as a response to technology specific challenges and the need to elaborate technology design obligations, the abovementioned Commission Implementing Decision would not produce results, which fall foul of the technology neutral aspect of the GDPR. Therefore, if there is room for interpreting the GDPR as a regulatory instrument allowing co-regulation, it actually helps the GDPR realise its ambition of being called a technology neutral law.

However, it remains to be seen if the model of digital identity management built on blockchain is able to assert legal compliance with the GDPR – a hurdle that returns to be overcome. The next part takes stock of this challenge.

B. GDPR and Blockchain Technology: Possibilities and impossibilities

1. Accountability

Given that both permissioned and permissionless blockchains rely on the multiplicity of nodes to ensure trust, pinpointing accountability seems to

[119] Irene Kamara, 'Co-regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation 'Mandate'' (2017) 8(1) European Journal of Law and Technology <http://ejlt.org/article/view/545/723>.

[120] Josef Falke and Harm Schepel (eds.), *Legal Aspects of Standardisation in the Member States of the EC and of EFTA*, vol 1 (H. S. A. Luxembourg: Office for Official Publications of the European Communities 2000), 181.

be a daunting task. In a short time-span, blockchain as a distributed ledger has posed a serious challenge for regulatory approaches that hinge on central intermediaries.[121] The simplistic definitions of data controller and data processor retained in the GDPR, although supplemented by way of onerous obligations to ensure data protection, are still not adequate to cover all entities involved in data processing in an interconnected technological environment.[122] The inability to pin-point a controller could have serious implications for the entire data protection framework in the GDPR and many of the data subjects rights would be rendered useless, e.g., right to data deletion, access and portability, security breach notifications and most importantly it would be difficult to coerce compliance with the stick of heavy fines.[123]

However, the situation is not that grim, given that currently the entities providing digital identity management on a blockchain are using permissioned blockchains. In this scenario, regulators can focus on either a technical system operator or consider the group of participating entities as joint controllers. The GDPR clarifies that in case of joint controllers they should have a transparent arrangement regarding the respective responsibilities for compliance and empowers the data subject to exercise her rights in the GDPR against one or all of the controllers irrespective of such an arrangement.[124] But if it were a case of public blockchain, the open and permissionless nature would mean that there could be an ever-growing army of nodes. Moreover the personal data is processed at every node each time a block is added in furtherance of a transaction, in such a situation the concept of joint controller responsibilities would fail to meet the requirement in Article 26(1) of having a transparent arrangement of responsibilities for compliance. The other option of choosing one or all the nodes as per Article 26(3) seems to be procedurally untenable.

Another variation of this challenge may manifest itself in the form of the data subject herself being the data controller because that is the aim of

[121] Matthias Berberich and Malgorzata Steiner, ‘Blockchain Technology and the GDPR: How to Reconcile Privacy and Distributed Ledgers’ (2016) 2 European Data Protection Law Review 422, 424.

[122] Neil Robinson et al, *Review of the European Data Protection Directive* (Cambridge 2009) <https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf> accessed 5 September 2017.

[123] Berberich and Steiner (n 121) 424.

[124] Article 26 GDPR.

the digital identity management platform –to return complete control to the data subject. However, it is probable that establishment offering these digital identity management services could be considered as 'gatekeepers' to the blockchain and find themselves bearing the brunt of compliance to GDPR. An entity like Sovrin or uPort could showcase willingness to comply with data protection principles by way of appointing a Data Protection Officer to carry out tasks specified under Article 39 of GDPR. Furthermore, as per the DIM model described previously, it is also possible to track the requests for access to personal data and the grant of the same by the data subject on the blockchain. This provides enhanced accountability and data provenance of personal data of data subjects utilising a DIM on a blockchain platform. The entities providing the DIM platform play a role in determining how the personal data of its users is processed, imparting to them characteristics of processors. Once clarified that the DIM platform provider is to be considered the controller and processor, veracity of permissions given by the data subject vis-à-vis the data usage can be authentically tracked on the blockchain and the platform provider be held accountable. This, in the author's opinion, strengthens the accountability principle.

2. Data Minimisation

This principle is a stalwart in the realm of data protection. Data minimization manifests itself in Article 5(1)(c) GDPR whereby the amount of personal data collected should be 'limited to what is necessary' to achieve purposes for which the data processed. Strangely enough it deviates from Article 6(1)(c) DPD, which provided that personal data must be 'relevant and not excessive in relation to the purposes for which they are collected and/or further processed'. In the DPD the provision was directed at ensuring minimality at the stage of data collection. However, the principle of data minimisation is also reflected in the purpose limitation provision whereby personal data shall be 'collected for specified, explicit and legitimate purposes and not further processed'.[125] Bygrave opines that rules encouraging transactional anonymity are also direct manifestations of the

[125] Article 5(1)(b) GDPR.

minimality principle.[126] The GDPR goes a step further in encouraging pseudonymisation of data. Digital identity management platforms built on blockchain would fall foul of the traditional understanding of the data minismisation principle whereby it focuses on minimization at the collecting and processing stage. This contradiction would arise from the very structure of blockchain technology where data is replicated on each node. At the same time, however, merely storing hashed pointers to the personal data and not the personal data itself on the blockchain would perhaps find favour with data minimisation. The requirement of transactional anonymity would be fulfilled by way of zero knowledge proof, whereby the data subject avails this feature on the digital identity management platform to return queries by the online service provider. In this manner, the online service provider would have access to bare minimum personal data, e.g, if YouTube wants to know that you are above 18 years to watch a particular video, it does not need to know your birthdate, a simple yes or no answer would suffice.

The relevance of using blockchain technology for a digital identity management platform manifests itself in reducing availability of personal data to online service providers. This squarely addresses the problem of profiling in the digital realm as well.

3. Control

As rapid technological developments mount new challenges for protection of personal data, the GDPR acknowledges the importance of trust in the digital economy. Recital 7 of the GDPR states the need for natural persons to have control over their personal data. In order to ensure this, the new framework goes out on a limb to broaden the scope of control and makes it more comprehensive.

The notion that consent could empower a data subject to have control over her personal data is based on a narrow view that control is limited to controlling the disclosure of data, in the author's opinion control is rather based on a broader right to personal autonomy. Throughout the GDPR, various provisions are intended to enhance control of the data subject over

[126] Lee A Bygrave, *Data Privacy Law: An Interntional Perspective* (Oxford 2014), 152.

her personal data. This is achieved by empowering the data subject with a strong portfolio of rights like right of access, right to be forgotten and right to data portability being the most important ones.[127] The author sees these rights as reinforcing individual control supported by the GDPR envisioning a heterogeneous set of normative and technological tools, for example, ways to ensure accountability and privacy by design mechanisms. Control also fosters autonomy by giving the data subject the ability to manage information about herself. Although the GDPR does not mention a 'right to identity', its provisions implicitly enable the data subject to control how she is perceived. This also fits well with the understanding that privacy is determined by the ability to control personal information.[128]

The digital identity management solution built on blockchain achieves the said goal of returning control over their personal data back to the data subjects in line with the reformed provisions of GDPR. It does so by providing the data subjects full control regarding who gets access to how much of their personal data and for what purposes it may be used. Therefore, the proposed model supports the data subjects to undertake privacy management in an effective manner. The technology aids them and eases the burden of maintaining their personal autonomy. It is a step in the direction of inculcating a culture of data protection rather than merely regulating data protection. The rights of data subjects are to be construed as a means to achieving higher degree of control rather than as ends.

4. Right to be Forgotten

Article 17 codifies one of the most important provisions enabling the data subjects to exercise personal autonomy with respect to their identities. The inclusion comes in the backdrop of the seminal *Google Spain* decision.[129] In this judgment, CJEU also highlights the perils of profiling. The provision attempts to regulate the privacy risks online in the age of 'perfect re-

[127] Articles 13, 17, 20 GDPR.

[128] H T Tavani, 'Privacy and the Internet' (2000) Boston College Intellectual Property & Technology <www.bc.edu/bc_org/avp/law/st_org/iptf/commentary/content/2000041901.html> accessed 8 September 2017.

[129] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ECLI:EU:C:2014:317

membering'.[130] Mitrou and Karyda opine that 'perfect and precise remembering affects the claim of individuals to live and act without leaving permanent traces or shadows'. This interferes with a crucial aspect of information privacy, in particular the right to informational self-determination and control of one's own personal data.

Article 17 encompasses the right of the data subject to erasure of her personal data and injunct the data controller from engaging in further dissemination of her data. This right comes into effect if:

a) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
b) the processing of personal data does not comply with the data protection framework; or
c) the data subject withdraws her consent or objects to the processing.[131]

It is pertinent to mention that this right to be forgotten does not apply retrospectively to the data already processed. Furthermore, this right imposes limited obligation on the controllers to 'what is technically feasible and does not require a disproportionate effort.[132] Therefore, it is important to bear in mind that right to be forgotten is not an absolute right that can always be requested by the data subject.

Right to be forgotten poses a big challenge for blockchain-based digital identity management solutions, given the immutable nature of the data stored on the blockchain. Although, immutability is the bedrock of blockchain technology, yet there are some technological suggestions to make the blockchain editable.[133]However, the author opines that it would be better to keep the feature of immutability intact if it comes at the cost of functionality that supports data protection. Regulators should not adopt a very restrictive interpretation and rather strike a balance between protecting privacy and the understanding of how technology shapes up. Article 35(1) of Germany's Federal Data Protection Act lends credibility to such

[130] Lilian Mitrou and Maria Karyda, 'EU's Data Protection Reform and the Right to be Forgotten: A Legal Response to a Technological Challenge' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2165245&rec=1&srcabs=2032325&alg=1&pos=10> accessed 8 September 2017.

[131] Mitrou and Karyda (n 130) 11.

[132] Article 19 GDPR.

[133] Accenture, 'Editing the Uneditable Blockchain: Why Distributed Ledger Technology Must Adapt to an Imperfect World' <www.accenture.com/t00010101T000000__w__/es-es/_acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf> accessed 7 September 2017.

an approach. According to Article 35(1), the controller can circumvent the obligation to erase personal data where erasure would be impossible or would involve a disproportionate effect due to the specific mode of storage. In such circumstances, the German Federal Data Protection Act proposes restriction of processing said personal data as per Article 18 of the GDPR. The German Act also relieves the controller oft he obligation to erase in the instance of erasure adversely affecting the legitimate interests of data subject. The utility of 'legitimate interest' provision in this regard is discussed at the end of this part.

Therefore, it is suggested that indefinite locking of data on an immutable blockchain should actually be considered compliance with other data protection principles in the GDPR rather than seeking to admonish it under the right to be forgotten. The insufficiency of legal instruments alone to deal with technological challenges has been buttressed already. It follows that the utility of the right to be forgotten will depend on its interpretation in the technological landscape and a forward looking approach similar to the one taken by Germany is advisable. It should not be the case that an isolated island of this right is created detached from the mainland that is the GDPR.

5. Right to Data Portability

This right is an internet-specific new right allowing the data subjects to exercise the freedom of changing who controls their data. In the current framework, for example, of data storage on the cloud, service providers spend considerable time and resources to push their registered users to further deepen their profiles. Once this is done, it is extremely difficult to extract their information from one platform and move it in entirety to another platform, making it extremely difficult to change service providers.[134] So far there has been neither the carrot nor the stick for ensuring system interoperability when it comes to personal data storage. However, the GDPR seeks to remedy this by specifically entitling the data subject to demand data portability in a commonly used and machine-readable format

[134] Paul de Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for The Protection of Individuals?' (2016) 32 Computer Law and Security Review 179, 189.

directly to the new controller of her choice.[135] However, what is peculiar is to hinge this right to portability to cases where the processing is done in furtherance of consent. This releases the controller from obligations to port data where the collection has happened on grounds other than consent, e.g., the good old legitimate interest ground for lawful processing contained in Article 6(1)(f) of the GDPR.

Further, there are arguments to tap the regulatory toolbox for governing data portability under competition law. [136] Koops also ponders over not employing competition as a regulatory tool, but laments that it may be due to the market structures of the data economy. However, he suggest that in light of dominance of certain multinational internet companies, a focus on providing market incentives for alternative providers with more privacy-friendly policies and default settings might be more helpful than command-based rules for data processing.[137]

However, when it comes to the digital identity management platform on a blockchain, it has inherent features of ensuring seamless interoperability because the data subject is in control of her personal attributes and can share them with whomever she chooses. In the rigid sense of the term data portability, whereby the data has to be on the servers of a new controller seems to be undesirable because one of the features of the digital identity management platform on blockchain is that nobody has access to the off-chain storage of the personal data and only pointers to the data are stored on the blockchain. Regarding portability to another DIM platform, it can be easily achieved in case of public blockchains by sharing the public key and pointing the new DIM service provider to the data, after which the said new DIM service provider would handle the access and use permissions.[138] In case of permissioned blockchains, portability may be achieved by way of the users downloading the data (using their private key) from one DIM service provider's platform and moving it to a new one. This

[135] Article 20(1) GDPR.

[136] De Hert and Papakonstantinou (n 134) 190.

[137] Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (TILT Law and Technology Preprint Publications 2014) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692> accessed 8 Spetember 2017.

[138] Blockchain Bundesverbrand, 'Blockchain, data protection, and the GDPR' (2018) <https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v 1.0.pdf> accessed 30 October 2018.

would have to be supplemented by a request to restrict processing of their personal data made to the previous DIM service provider.

6. Data Protection by Design

In furtherance of its technology neutrality, the GDPR mandates data protection by design.[139] The Article 29 Working Party had argued for the induction of data protection by design as a legal obligation in order to take technological data protection into account at the planning stage of platforms dealing with personal data.[140] The objective of data protection by design is that 'the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'.[141] This provision provides the stimulus for innovation in the field of technical data protection by design principles. At the same time, the technologies do not have a free pass and ought to provide data protection as envisaged in the GDPR framework. Data protection by design seeks to encourage the integration of technical and organizational measures into the business models of data controllers. The role that technical standards can play in achieving data protection by design has been covered in the part discussing technology neutrality of the GDPR.

It follows from the above discussion that although the digital identity management platforms claim to provide heightened level of protection for personal data, these claims have to be tested regarding their compliance with the obligations set forth in the GDPR. The previous points in this part of the thesis explain how provisions like data minimisation and right to be forgotten interact with a blockchain-based solution for personal data protection.

One way of reconciling all the abovementioned issues is to take into consideration the 'legitimate interest' as a legal basis for processing personal data. This strikes a cord with the other aim of the GDPR, i.e., ensure free movement of data and is the saving grace for data controllers.[142] The EU jurisprudence is replete with cases emphasizing that interferences with

[139] Article 25 GDPR.

[140] Hilderbrandt and Tielmans (n 102) 516.

[141] ibid 517.

[142] Lee A Bygrave, *Data Privacy Law: An Interntional Perspective* (Oxford 2014), 121.

the rights to privacy and data protection must be strictly proportionate to the aims pursued.[143]Moreover, the *Google Spain* decision requires that the balancing activity for establishing 'legitimate interest' must take note of the data subjects' rights arising from Articles 7 and 8 of the Charter.[144] In the GDPR Article 6(1)(f) codifies the 'legitimate interest' route to lawful processing. It considers processing done for legitimate interests pursued by the data controller to be lawful. The *Breyer* decision offers some insight regarding the interpretation of 'legitimate interests'.[145] According, to this decision a service provider's activity of collecting and processing personal data without the data subject's consent can be considered to be lawful if such collection and processing is necessary to facilitate the use of those services by the data subject.

In furtherance of the interpretation of 'legitimate interest' in the *Google Spain* and *Breyer* decisions, it is possible to reconcile a blockchain-based solution for protecting personal data with the GDPR. The underlying technology for the digital identity management platforms suggested in this thesis entails significant difficulties for compliance with the prevailing understanding of the right to be forgotten and the accountability principle. Yet it is possible to take recourse to the very structure of the blockchain technology, which imparts the high level of data protection to the said platforms. Therefore, in as much as the collecting and processing of personal data done by these platforms is necessary for the functionality of these platforms in protecting personal data of the users, such activities can be considered lawful irrespective of the challenges posed by other provisions in the GDPR. It is important to note that legal rules pertain to normativity rather than regularity and should 'work as standards for interaction that create legitimate expectations', leaving scope for interpretation.[146]

[143] CJEU, joined cases C-465/00, C-138/01 and C-139/01 (*Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk*), judgment of 20 May 2003, ECLI:EU:C:2003:294, para. 86; case C-275/06 (*Productores de Música de España (Promusicae) v Telefónica de España SAU*), judgment of 29 January 2008, ECLI:EU:C:2008:54, para. 54; joined cases C-92/09 and C- 93/09 (*Volker und Markus Schecke GbR, Hartmut Eifert v Land Hessen*), judgement of 9 November 2010, ECLI:EU:C:2010:662, para. 72.

[144] *Google Spain* (n 129).

[145] Case C –582/14 *Commission v. Breyer* ECLI:EU:C:2017:563.

[146] Hilderbrandt and Tielmans (n 102) 518.

Here is a table illustrating the extent to which reconciliation of digital identity management platforms built on blockchain with GDPR is possible.

Table 3: Reconciliation Chart

Features of Blockchain powered DIM	**GDPR Provisions**	**Possibility of Reconciliation**
Decentralised transaction storage	Accountability	Possible
Replication of data over nodes	Data minimisation	Possible
Querying on a DIM platform	Control by Data Subject	Achieved by the technology
Immutability	Right to be forgotten	Requires flexible interpretation
Locking up of Data	Right to Data portability	Possible
Core features of blockchain	Data protection by design	Achieved by the technology itself