Legal Standards Governing Data Protection in Europe and Potential Sources of Legal Transplants in Macau SAR

M.P.Ramaswamy

University of Macau, Macau SAR

DOI: https://dx.doi.org/10.47772/IJRISS.2021.5637

***Abstract* – In the past, both Hong Kong and Macau SARs have been influenced by the legal traditions of European origin. Since the establishment of the two SARs, how normative developments in these two jurisdictions compare with the evolution of specific legal standards in Europe continue to interest academic scholars and legal professionals. This paper aims to analyse the evolution of data protection standards in Europe and examine how its more recent transformation seeks to extend its regulatory reach upon data transfers beyond its borders. The paper will examine the European GDPR closely to determine its unique characteristics, which has the potential to drive the formation of data protection legal standards in other jurisdictions. Being one of the jurisdictions that has been influenced by certain European legal traditions in the past, Macau SAR's interest in assessing the relevance of European data protection standards as a potential source of legal transplants in developing the domestic regulatory framework is natural. Therefore, the paper will examine how the Macau domestic legal standards governing the protection of personal data have been influenced by European standards. It will also examine the potential of the GDPR standards as a source of influence for the future development of data protection standards in Macau. The paper concludes with an argument that beyond any comparative analysis with other regional experiences like the European GDPR, Macau SAR should consciously seek to increase harmonisation of its data protection regimes viz a viz other international and regional markets like the PRC and Hong Kong SAR to facilitate the aspiration of the regional economic integration in the Greater Bay Area in southern China.**

***Keywords*–Data protection law, European Legal Standards, GDPR, Macau, Greater Bay Area**

I. INTRODUCTION

Towards the close of the twentieth century, the world witnessed a historical return of Hong Kong and Macau to the People's Republic of China (PRC). These jurisdictions, which were under the erstwhile administration of two European nations, namely the United Kingdom (UK) and Portugal respectively, have since been conferred the status of Special Administrative Regions (SARs) of the PRC, enjoying various political, economic, legal, and social autonomy. In the legal field, in particular, the SARs have enjoyed legislative and judicial freedom manifesting distinct characteristics between themselves as well as that of the PRC. The legal standards in various fields of governance in the two SARs have been developed by their respective autonomous legislative mechanisms, and to cater to the needs of their societies, the SAR judiciaries have independently exercised the interpretative powers. Moreover, it is relevant to note that Hong Kong and Macau SARs, which have been influenced by the legal traditions of the UK and Portugal, respectively, have continued to retain the characteristics of the legal systems and various laws inherited from their previous administration. This is made possible by virtue of the principle of continuity, agreed between the concerned sovereign states under the related historical declarations governing the handover of the two jurisdictions to the PRC (Sino-British Joint Declaration 1984 and Sino-Portuguese Joint Declaration 1987). In addition, the constitutional legal instruments implementing the declarations, namely the Hong Kong Basic Law and Macau Basic Law, have reinforced the continuity principle through various rights and guarantees.

An important question in this context, namely to what extent the legal evolution in Hong Kong and Macau compares with or is influenced by the legal developments in the UK and Portugal, respectively, raises curiosity among jurists aiming to assess various legal standards in the two SARs. As this intriguing question cannot be answered in general and needs investigation in specific fields of legal governance, this paper aims at assessing the key characteristics of the legal regimes governing data protection in Europe. The second part of the paper closely assesses the key milestones in the European data protection regimes, including the European Union (EU) Directive on Data Protection 1995 and the General Data Protection Regulation (GDPR), which are the bedrock of the legal standards governing data protection regimes in the UK and Portugal albeit the recent exit of the former from the EU.

The paper will briefly analyse the specific legal standards governing data protection in Macau SARs in light of the findings of the GDPR. It will also examine the extent of influence of the European legal standards upon the domestic legal standards governing data protection in the Macau SAR and identify the relative strength and weakness of data protection regimes in Macau SAR. The final part of the paper arguesfor the need to harmonise the legal standards of data protection in line with the European developments and with regional markets, including that of the PRC and Hong Kong SAR. This is recommendedto ensure that Macau SAR canserve its role in facilitating trade with the outside world and achieving an effective economic integration in the Greater Bay Area (GBA). The significance of this study mainly pertains to the systematic analysis of the evolution of the European legal standards

governing personal data protection and its maturity as the GDPR creating potential influences within and outside Europe.

Further examination of the effect of the European legal standards externally upon the Macau SAR and how any future reference to the European standards need to be balanced with other international and regional developments adds more significance. The tenacity of the GDPR and the firm judicial interpretations nullifying the bilateral arrangements like the safe harbour and privacy shield arrangements have caused problems for data operators within and outside Europe regarding how to ensure strict compliance. Tracing the origin and evolution of specific data protection standards in Europe and their influences outside Europe is expected to provide particular insights of practical significance in addressing the problem. Although the study seeks to examine the impact of the European standards externally upon Macau SAR, to what extent the GDPR will command a similar influence like the Directive is a challenging propositionto predict. The future goals in this direction need to examine the relevance of specific data protection standards in the GDPR for Macau SAR in a comparative perspective with other international and regional standards.

II. THE EUROPEAN EVOLUTION IN DATA PROTECTION AND THE ESTABLISHMENT OF THE FUNDAMENTAL LEGAL STANDARDS GOVERNING PERSONAL DATA PROTECTION.

The European data protection initiative was one of the pioneering efforts in the world that sought to protect personal data legally. Although protection of the broader right to privacy in Europe could be traced earlier, the concrete effort in providing legal protection for the processing of personal data was first introduced by the Council of Europe (COE) in the early eighties. The European Convention on Human Rights 1950 (European Convention 1950) guaranteed the right to privacy[1] in unequivocal terms and recognised exceptions only in a prescribed set of circumstances[2], which arguably served as an inspiration for the COE in aspiring for a specific data protection Convention. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 (COE Convention 1981) is the forerunner in data protection in Europe. Although the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 (OECD Guidelines 1980) just preceded the COE Convention 1981, it was an instrument lacking binding effect and was mainly meant to promote protection in a transboundary context.

The COE Convention 1981 was aimed at protecting an individual against any abuse resulting from the collection and process of personal data and at the same time regulating the transfer of such data across borders. Beyond the general protection, the COE Convention 1981 is evidently the genesis of some of the key features of the modern legal regimes governing personal data, such as the prohibition of collection and process of sensitive personal data without sufficient safeguards, the need to guarantee equal protection standards before the transfer of data to a foreign jurisdiction, the right of the data subject to seek the disclosure of personal data collected and the right to correct the same, etc. It is intriguing to note that the need for the COE Convention 1981 was justified in the light of the increased automation in the processing of personal data as early as the eighties and the preponderance attached for upholding the right of privacy of individuals in that time. Apart from enhancing its reach through broad definitions like what amounts to automatic processing and who will qualify as the controller of a data file, the COE Convention 1981 extended its scope to both the public and private sectors involved in the automatic processing of personal data. However, freedom was provided to the State Parties to limit the scope of application of the Convention or to enhance its application beyond individuals and personal data not subjected to automatic processing. (Article 3 (2), COE Convention 1981).

The COE Convention 1981 has been the forerunner in establishing some of the fundamental legal principles governing data protection that were contemplated as a minimum standard (Article 11, COE Convention 1981). The influence of the legal tenets laid down by the COE Convention 1981 upon subsequent normative developments in Europe cannot be disputed. The Convention prescribed various requirements relating to obtaining, processing, storing, using, updating, and preserving data in defining the principle governing the quality of personal data that are processed automatically. The principle on data security warranted measures to ensure protection against destruction or loss of data or certain types of unauthorised acts. The Convention also established principles providing various other safeguards for the data subjects, including the right to ascertain the existence of personal data files and obtain different allied information and the right to rectification or erasure and related remedies.

The Convention only permitted derogation from key principles on exceptional grounds specifically recognised like state security and public safety. Restrictions regarding certain rights were recognised for statistical purposes or scientific research. However, the regulation of transfer of personal data beyond national jurisdictions under the COE Convention 1981 was limited in scope, as it was foreseen only in the context of transfers involving the automatic processing of data. In addition, the restrictions of cross-border transfer have been prescribed as an exception rather than as a rule when the transfers involved jurisdictions within the state parties to the Convention. Therefore, prohibiting or requiring authorisation to transfer personal data between or involving the territories of the state parties have been permitted only in prescribed circumstances. To ensure effective implementation of the safeguards, the Convention not only obliged state parties to provide mutual assistance to each other but also mandated them to aid

[1] The right mandated respect to private and family life of individuals including their home and correspondence. See Para 1, Article 8, European Convention on Human Rights, 1950.

[2]Exceptions are recognized only on the grounds of national security, public safety, state's economic well-being, disorder or crime prevention, protectionof health or morals, or the rights and freedomsof other individuals.

eligible data subjects residing abroad. The creation of a joint consultative committee involving the representatives of the state parties, with one of the aims to facilitate or improve the application of the Convention, further enhanced the means to realise and enhance the goals of the COE Convention 1981.

Deriving the concrete experiences in legally protecting the right to privacy and personal data protection, the European Union made a significant initiative in the mid-nineties to direct its member states to guarantee legal protection in their domestic regimes. The EU Directive on the protection of individuals regarding the processing of personal data and on the free movement of such data 1995(The EU Directive or 1995 Directive)[3]was a legal initiative during the early years of the emergence of the world wide web. The EU Directive could be seen as a timely EU response to the threats the personal data starting to emerge from the modern information technologies. It is arguable that such a timely response was made possible because of the development and maturity of the specific fields right to privacy and personal data protection in Europe, as well as the related jurisprudence resulting from the interpretation of the related legal instruments since the mid of the century. For example, the interpretations of the European Court of Human Rights pertaining to the right to privacy and freedom of expression[4]in the European Convention 1950 and the balance between the two rights[5] as well as the jurisprudence on the COE Convention 1981 have certainly provided a rich experience for the EU in enacting the new Directive.

Over the period, specific legal standards relating to personal data protection have gained prominent recognition, making it easier for the EU Directive to incorporate them within its corpus without many challenges. Several standards in this regard are worth noting for any legal transplant projects seeking to emulate the European experience. These standards could be classified into different categories based on specific issues or stages relating to the collecting and handling of personal data. Such legal standards could be grouped into various categories, including those relating to the purposes of collecting personal data, the manner of collection, the quality of data, the manner of storage of data, types of use of data, recognition of the rights of the data subjects,etc. To facilitate the free flow of data between member states, the EU Directive sought to achieve harmonisation of data protection legal standards among the member states. In developing the Directive, the previously established legal standards like the COE Convention 1981 served as an important source of reference.

The Preamble of the EU Directive is evidence of how balancing personal data protection with other interests of the society and various stakeholders involves numerous issues and why striking a proper balance would be a complex process. Opening with an emphasis on the broader objectives of the European Community and the mandate to uphold human rights, the 1995 Directiveset out some of the key values or interests that need to be respected by any data processing system. Such systems should respect fundamental rights and freedoms, including specifically the right to privacy, which was given the preponderance followed by specific purposes that need to be balanced, namely contribution to economic and social progress, expansion of trade and individual wellbeing[6]. The preamble then emphasised that the quintessential characteristics of the internal market of the EU, namely the free movement of goods, services, people, and capital required a fine balance between free movement of data and protection of fundamental rights of individuals. The preamble proclaimed other relevant values and principles in another 69 distinct paragraphs, demonstrating the numerosity and diversity of issues at stake in personal data protection.

The objective of the EU Directive also reiterated the values of protection of fundamental rights and free flow of personal data among its member states. Unlike the COE Convention, the scope of application of the EU Directive was extended to both the processing of personal data using automatic means as well as means that do not use automatic processing[7]. Being a directive and having recognised the need for its implementation through national laws of the member states, it prescribed different circumstances relating to the establishment of the controller of personal data when the application of a specific national legal standard should take place. The substantive provisions of the EU Directive prescribed as the general rules governing the lawfulness of personal data processing prescribe various categories of legal standards governing specific issues or stages involved in the personal data processing.

The set of issues or stages relating to which legal principles and standards were prescribed includes principles of data quality, criteria for legitimate data processing, distinct rules governing certain special categories of data, duty to provide different types of information to a data subject, rights of the data subjects, grounds for exemptions and restrictions from certain obligations and rights, measures to ensure confidentiality and security in processing personal data, notification obligations to a supervisory authority, etc. To ensure the effective implementation of the substantive obligations and rights recognised under the EU Directive, it imposes various liabilities and sanctions for violations and provides relevant judicial remedies. Contemplating the situations of personal data transfers to countries outside the Union, the EU Directive prescribed the principles governing such transfers and addresses certain situations of derogations to those principles by prescribing relevant measures to be taken by member states under such circumstances. The EU Directive prescribed certain codes of conduct for the proper implementation of relevant legal standards. The creation of a supervisory authority to oversee the implementation and a working party on the subject matter was also directed.

After the EU Directive, when the Charter of Fundamental Rights of the EU was promulgated in 2000 (The EU

[3] See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.
[4]See Article 10 (1), European Convention on Human Rights, 1950.
[5]See Article 10 (2), European Convention on Human Rights, 1950.

[6]See Directive 95/46/EC, Oct.24, 1995, Preamble, Para.2.
[7] The non-automatic processing means are recognized as part of an existing or intended filing system. See Article 3, para 1,of the Directive 95/46/EC.

Charter), as the protection of personal data has already gained wider recognition in various EU instruments like the COE Convention and the Directive, the right of personal data protection achieved an explicit recognition. The EU Charter, while recognising the right for everyone, mandated fair processing of personal data for the specified purposes only. Moreover, such processing can only be done based on either the consent of the data subject or legitimate grounds recognised by law. The rights of the data subjects to access and rectify their data are categorically recognised[8]. Finally, the Charter requires that compliance with the above legal standards should be ensured through appropriate control by an independent authority. Following the Charter, the next major European instrument sought to protect personal data in the context of electronic communications.

The European Directive on Privacy and Electronic Communication (EU Directive 2002) prescribed specific rules to safeguard the privacy and confidentiality of individuals personal data in public electronic communication services[9]. The EU Directive 2002 was aimed at the harmonisation of relevant legal standards in the member states governing the right to privacy arising in the context of the processing of personal data in the electronic communications sector. It also sought to harmonise the rules aimed at ensuring the free movement of personal data, electronic communication equipment and services.The EU Directive 2002mandates the providers of public electronic communication to take appropriate measures to enhance security and the member states to introduce laws to ensure the confidentiality of the communications. It requires the traffic data relating to the subscribers and users of the services to be erased or made anonymous beyond a certain period or purpose. Similarly,a restriction is also imposed on the processing of location data of the subscribers or users, which are subjected to anonymisation or consent and permitted only to the extent and duration needed to provide any value-added services. Unsolicited communications except with the prior consent of the subscribers are not permitted under this Directive. In the end, the EU Directive 2002 recognises the application of some of the provisions of the 1995 EU Directive for certain matters, including judicial remedies, liabilities, and sanctions.

Finally, it is very relevant to take note of the significance attached to the protection of personal in Europe with reference to the case of invalidation of the attempt of the EU and its member states seeking to legalise data retention in certain circumstances. The EU introduced the Data Retention Directive in 2006 that required relevant service providers to retain traffic and location data belonging to individuals or legal entities for a prescribed period for the purpose of prevention, detection, investigation, and prosecution of serious crimes. Although the purpose seemed justifiable and it did not mandate the retention of the actual communication itself, the Directive was declared void and invalid by the European Court of Justice (ECJ)[10]. The key grounds on which the Directive was squashed included serious interference in the right to privacy and personal data protection of individuals exceeding the relevant proportionality limits. The case demonstrates how the European legal standards governing personal data protection and its interpretations have kept the right to privacy and personal data protection at a very high pedestal, whereby even potential transgressions of the relevant rights are not tolerated even if they arise from the seemingly justifiable acts of the states. Such jurisprudence, as well as the long experience in enacting and implementing personal data protection, provided further impetus for the European Union to elevate the protection mechanism further. Consequently, the initiative to introduce a comprehensive EU Regulation for data protection that is directly enforceable in the member states began, which ultimately resulted in the promulgation of the GDPR in 2016 that entered into force in 2018.

III. THE REACH OF THE GDPR: THE INTERNAL AND EXTERNAL DIMENSIONS

The GDPR specifically defines its territorial scope to encompass personal data processing, when it is done in the 'context of the activities' of an establishment of a data controller or a processor in the Union, but irrespective of the fact whether the underlying process actually takes place within or outside the Union. By virtue of these provisions, the GDPR will become applicable to all digitalisation involving personal data by the establishments in the Union, even when they outsource related data processing from outside the Union[11]. This will be particularly relevant for several service providers like the banking and insurance in the EU, who have integrated foreign data processing and call centres as part of their digitalisation strategy. Interestingly, the very location of the data controllers involved in digitalisation within the EU mandates compliance with GDPR irrespective of whose personal data they process.

If any data controllers or processors from outside the Union offer goods and services to the data subjects in the Union or monitor their behaviour within the Union and process their personal data, it will attract the application of the GDPR. So foreign establishments engaged in digitalisation involving personal data of the EU data subjects, while targeting EU markets or monitoring EU consumers, should be cognizant of the potential application of the GDPR[12]. In such circumstances, the data controllers or the processor are required to designate a representative within the Union for ensuring compliance with the GDPR. Nevertheless, such designation of a representative by itself does not absolve the

[8]See Charter of Fundamental Rightsof the European Union(2000/C 364/01), Article 8 (2).

[9]Directive on Privacy and Electronic Communications 2002, 2002/58/EC.

[10]See *Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources and others*, European Court of Justice, Grand Chamber, April 8, 2014.

[11]For a specific analysis of the implications of GDPR for companies providing services based on personal data see Christina Tikkinen-Piri, Anna Rohunen, and Jouni Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", *Computer law and security review* 34, no.1 (2018): 134.

[12] See Kurt Wimmer, "Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers", *Syracuse law review* 8(2018): 547

designating data controllers or processors from potential legal actions pursuant to the GDPR[13].

Finally, the application of the GDPR is foreseen when personal data processing is carried out by a data controller established in a place outside the Union but where the law of a member state becomes applicable by the operation of public international law[14]. The scope of this application is particularly relevant for diplomatic missions from EU member states established in foreign territories that process personal data. As digital processing of personal data is commonly adopted by such missions, identification of relevant duties under the GDPR and compliance are essential. Such compliance can also serve as evidence of best practice for other local data controllers processing personal data of EU data subjects and who are subjected to the application of the GDPR, as discussed earlier.

From the above analysis, it is obvious that firstly, the GDPR becomes applicable to all data controllers or processors established in the Union or established outside the Union but are governed by the law of a member state. In such cases, the processing of anyone's personal data will attract the application of the GDPR. Secondly, the application of the GDPR will be triggered even when a data controller or processor is not established in the Union, but they should be involved in the processing of personal data of EU data subjects while offering them goods and services or monitoring those data subject's behaviour in the Union. Therefore, it is evident that the GDPR could become relevant for any digitalisation process involving personal data if any of the inextricable links with the EU discussed earlier exists.

The GDPR, at the very outset, stands out in terms of enforceability. Unlike the pertinent previous EU instrument governing the matter, namely the Data Protection Directive 1995 ("the 1995 Directive"), the GDPR is directly enforceable in the EU member states. This not only enhances the enforceability of the data protection standards but also minimises potential variations and related concerns about national implementations in individual member states. This distinct advantage of the GDPR can only be appreciated in hindsight of the implementation experience of the 1995 Directive, which reveals some serious challenges faced by the EU[15]. The review of the implementation history of the 1995 Directive reveals that the major concerns relating to lack of implementation by the member states continued to exist for several years even after the Directive came into force. In addition, instances of incorrect, divergent, incomplete, deficient, and unsatisfactory implementation were also found. This has prompted the European Commission to initiate judicial action at the European Court of Justice (ECJ) against some prominent members like Germany, France, Netherlands, Ireland, and Luxembourg[16].

In certain states, concerns about incorrect implementation were raised. Such implementation was found to have caused restrictive effects in the processing of personal data more than what was intended by the 1995 Directive[17]. This created a subtle obstacle to the free circulation of personal data even between the EU member states and arguably defeated the very objective of the 1995 Directive[18]. Even in cases where there was proper and correct national implementation, divergences among different national implementations were found[19]. The divergence caused adverse impact on transactions of the member states with third countries outside the Union and had internal implications within the Union[20]. Member states were sometimes found to have incomplete or unclear implementation of certain provisions of the Directive, which triggered regulatory rigidity. Some member states suffered deficient implementation of certain crucial standards of the 1995 Directive. For example, the deficiency in national implementation of the relevant applicable law provisions prescribed by the Directive had created conflicts of law, causing ramifications for the internal market of the Union[21]. Concerns regarding the unsatisfactory implementation of certain provisions of the Directive that prescribed the principles of data quality and criteria for legitimate processing of data were also expressed[22].

The above-discussed challenges could be attributed to the EU's choice of using a new regulatory instrument (instead of amending the 1995 Directive) in its recent introduction of more advanced personal data protection standards through the GDPR. Although the GDPR does not require specific enactment of national legislation in the member states to implement its key legal standards, it still provides room for member states to fill certain gaps that are intentionally left for providing the necessary flexibility to accommodate specific national sensitivities[23]. For example, the GDPR recognises the right of the member states to prescribe specific rules under their national laws for the processing of

[13] See Article 27 of the GDPR.

[14] See Article 3(3), GDPR.

[15] Challenges and resistance were also faced even at the preparatory and passing stages of the Directive. For relevant discussion see Spiros Simitis "From the Market to the Polis: The EU Directive on the Protection of Personal Data", *Iowa law review*, 80 (1994-95): 445.

[16] In the case against the Luxemburg, the complaint also resulted in the condemnation by the ECJ. See Commission of the European Communities, *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, Brussels, 15.5.2003, COM (2003) 265 final, pp. 27 ("First Report on the Implementation of the 1995 Directive") available online at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0265&from=EN.

[17] Ibid at p.10.

[18] One of the principal objectives of the 1995 Directive was the removal of any barriers to the free movement of personal data between the EU member states. See Article 1(2) of the Directive 95/46/EC, Official Journal L 281, 23/11/1995 P. 0031 – 0050 available online at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

[19] For example, divergence was specifically found among number of member states while implementing Articles 10 and Article 11 of the 1995 Directive, which prescribed the duty of the controller of data to provide relevant information to the data subjects in different scenarios.

[20] The divergence in question was related to Article 25 and 26 of the Data Protection Directive 1995.

[21] See the First Report on the Implementation of the 1995 Directive at p.17.

[22] See Articles 6 and 7, Data Protection Directive 1995.

[23] Julian Wagner and Alexander Benecke, "National Legislation within the Framework of the GDPR" *European data protection law review* 2 (2016): 353.

the personal data of employees in an employment context[24]. Moreover, the member states are provided with the freedom to define or modify certain provisions. For example, the GDPR, while prescribing the minimum age of a child as sixteen years to provide consent for the processing of personal data in the context of information society services directly offered to a child, recognises the right of the member states to lower the age of consent, albeit subject to a minimum limit of thirteen years[25]. Member states have taken advantage of these flexibilities provided in the GDPR and have enacted relevant national rules on matters in which they enjoy freedom, like the new Data Protection Act 2018 of the United Kingdom[26].

The analysis reveals that any relevant stakeholders, including those from Macau facing the GDPR, should be aware that the flexibilities provided to member states to vary or fill the gaps of the regulation could trigger the application of distinct legal standards while dealing with specific member states. Moreover, it is equally critical to note that the new EU data protection regimecould still give rise to more stringent deterrent measures being introduced by specific member states. For example, the UK Data Protection Act 2018, going beyond the GDPR, has introduced a new offence of re-identification of information from de-identified personal data without the consent of the controller de-identifying the data. Relevant stakeholders should take note of this potential unique offence while dealing with the UK and take appropriate measures. This is because of the possibility that prosecution could result not only in cases of knowingly re-identifying de-identified personal data but also recklessly doing so[27].

In assessing the key features of the GDPR, a comparison with the 1995 Directive to identify key changes and additions is inevitable. Such an approach will not only categorically indicate the improvements the GDPR seeks to achieve but also indicate how relevant data controllers and processors within and outside the EU should adapt to the changes effectively to ensure compliance. For example, a systematic comparison of the legal provisions and standards relating to the scope of application and jurisdiction in the GDPR and the 1995 Directive indicates the extraterritorial implications of the emerging EU data protection standards. At the same time, the dual objectives of the two instruments, namely the protection of personal data and breaking the barriers to the free movement of personal data, remain the same[28].

The GDPR prescribes expanded provisions enhancing its territorial and material scope. The scope of application of the 1995 Directive was mainly focused on the processing of personal data generally when a controller or processor of the data is established in the Union. However, as specifically discussed earlier, the GDPR extends its tentacles further, whereby it becomes applicable even when data controllers or processors are not established in the Union[29]. However, regarding the material scope of application, the GDPR does not deviate much from the Directive, albeit some differences are visible in excluding the material scope to the processing of personal data under the provisions of specific legal instruments of the Union. Comparatively, the Directive contained an additional ground limiting its material scope, namely when the processing of personal data was done in the context of Title VI of the Treaty of the European Union. The GDPR, on the other hand, recognises two new grounds limiting its material scope, namely the processing of personal data by the Community institutions and bodies subjected to the EC Regulation 45/2001 and by the E-commerce intermediary service providers subject to the Directive 2000/31/EC.

The GDPR provides an expanded definition of 'personal data' that includes information of any identified or identifiable natural person. The identifiability of a natural person is widely defined, covering the possibility of both direct and indirect identification using various identifiers. The list of indicative identifiers includes certain elements that are particularly relevant to digitalisation operations, namely location data or an online identifier[30]. Various other definitions under the GDPR includes activities or operations that could typically arise in the context of digitalisation. Some of those activities are recognised as part of the definition of the terms like processing, profiling, pseudonymisation, consent and personal data breach[31]. For

[24] See Article 88 of the GDPR. While providing the leeway for the member states, it is important to note that the GDPR mandates such enacted rules to guarantee certain safeguards relating to the human dignity, legitimate interests and fundamental rights of the data subjects with due regard to specific aspects of handling of data including transparency in processing standards and transfer of personal data.

[25] See Article 8 of the GDPR.

[26] In this context, the UK legislation has taken advantage of the flexibility and prescribes the age of a child capable of giving a valid consent as thirteen albeit specifically excluding the provision of preventive or counselling services from scope of the information society services offered directly to a child. See Section 9, Data Protection Act 2018.

[27] See Section 171, Data Protection Act 2018. The distinction of UK Act in comparison with the GDPR can also be found in case of the use of relevant terminologies. The GDPR refers to 'pseudonymisation of personal data', which signifies a process whereby personal data could not be attributed to a specific data subject without the use of additional information that is not only kept separately but also subjected to measures ensuring non-attribution to an identifiable natural person. On the other hand, the UK Act uses the term 'de-identified personal data', which is broader in scope enabling the scope of the Act to encompass any attempt to re-identify the personal data subjected to the process of anonymisation (could be seen as analogous to criminalization of acts circumventing any technological measure introduced to protect intellectual property in digital works). See Mark Phillips, Edward S. Dove, and Bartha M. Knoppers, "Criminal Prohibition of Wrongful Re-identification: Legal Solution or Minefield for Big Data?" *Journal of bioethical inquiry*14, no.4 (2017):527.

[28]Although the language of the GDPR regarding the specific right of the data subjects to be protected is phrased relatively broad. While the GDPR aims to guarantee a general right to the protection of personal data, the 1995 Directive sought to protect the specific right to privacy with respect to the processing of personal data. See Article 1(2) of the GDPR and Article 1(1) of the Data Protection Directive 1995.

[29] For a systematic discussion on the extensive territorial scope of the GDPR application see Merlin Gomann, "The new territorial scope of EU data protection law: Deconstructing a revolutionary achievement" *Common market law review*, 54, no.2 (2017) 567.

[30] The other elements include typical identifiers like name and identification number of natural persons. Moreover, the GDPR recognizes an expanded list of factors defining specific attributes of a natural person could also serve as identifiers. It is noteworthy that digitalization involves the processing and storage of data that commonly includes such typical identifiers and specific attributes. As a result, the related digitalization would inadvertently be classified as processing of personal data and fall within the purview of the GDPR.

[31]See Article 4 (2), (4), (5), (11) and (12) of the GDPR.

example, the definition of the term processing includes a range of 'operations on personal data using automated means.' Profiling is defined to include any form of 'automated processing of personal data' for evaluating personal aspects relating to a natural person as well as 'any analysis and prediction' of those aspects. Similarly, the definition of pseudonymisation requires that any additional information necessary to attribute data to a specific data subject should be kept separately and be subject to 'technical' and organisational measures. Moreover, the GDPR prohibits the processing of some special categories of personal data, like those revealing racial or ethnic origin, political opinions, religious beliefs, genetic information[32], data concerning health or sexual orientation etc., except under prescribed circumstances[33]. Using digital platforms to conduct predictive analysis using personal data may transgress such limitations, and enterprises engaged in digitalisation should clearly demarcate such data to avoid violation of the GDPR prohibitions.

The term consent is defined as the indication of a data subject's wish in a prescribed manner expressed through a statement or 'a clear affirmative action' to signify the agreement to process their personal data. Finally, the term personal data breach is defined as 'a breach of security' causing destruction, loss, alteration, unauthorised disclosure, or access to personal data. Digitalisation entities should pay attention to the above-discussed actions or operations forming part of specific definitions in the GDPR. This is because of the possibility that their potential engagement in similar activities could satisfy the definitions and trigger the application of the GDPR. In addition, a clear understanding of the scope of the definitions of certain key stakeholders related to personal data processing, namely data subject, data controllers, data processors, the recipient and third party, is crucial for entities involved in digitalisation[34].

Like the assessment of the scope of application and definitions, a review of the substantive provisions of the GDPR will benefit stakeholders to achieve better compliance with relevant regulatory standards. In this regard, the question of 'lawfulness of personal data processing' under the GDPR is one of the key standards. The GDPR prescribes that processing of personal data will be lawful only under prescribed circumstances involving the consent of the data subject, performance of a contract with the data subject, compliance with a legal obligation facing data controller, the protection of vital interests of the data subject or another natural person, tasks of public interest or exercise of official authority of a controller, and legitimate interests pursued by the controller or by a third party subject to some exceptions[35]. Entities handling personal data governed by the GDPR should pay special attention to conditions and qualifications attached to the specific grounds of lawfulness. For example, the ground of consent requires that the data subject should be related to one or more specific purposes. Therefore, obtaining a very general consent of a data subject will not protect entities using personal data for a wide range of purposes that are made feasible by digital technology. Similarly, the processing of personal data under the ground of necessity of contractual performance may not always justify the use of digital means to process such data, especially when alternative conventional forms of processing should have been preferred to protect the security and integrity of the underlying data.

When the lawfulness of the personal data processing is sought to be justified based on consent, the data controller should be able to prove the consent and at the same time enable the possibility for the data subject to withdraw the consent any time. Moreover, to determine whether the consent is given freely, the GDPR calls for an enquiry to ascertain whether the relevant contract to provide a service by the data controller is conditional on the consent to process personal data that is not essential for the performance of the underlying contract. The entities offering services in digital form should design their platforms to enable withdrawal of consent and ensure that consent obtained pertains to the personal data that are indispensable for the rendering of the digital service. Similarly, when data controllers handle personal data relating to a child while offering information society services directly to them, they should seek and ensure parental consent. To discharge the onus ofmaking reasonable efforts to verify and ensure parental consent, the digital service providers should pay specific attention to the importance attached to the 'technology available at their disposal' by the GDPR[36].

Enterprises engaged in personal data processing should also be wary of various rights of the data subjects enshrined and protected under the GDPR. Firstly, it is important to identify the specific obligations imposed upon the data controllers to ensure the effective exercise of the recognised rights by the data subjects, including those relating to the facilitation of relevant communications and supply of required information in a transparent manner[37]. The obligation of data controllers to provide the prescribed set of information is recognised when the personal data is collected from the data subjects directly, as well as in circumstances where the personal data obtained for processing was not from the data subjects. Therefore, digital service providers should not be under the illusion that the right of a data subject to obtain information may not arise when the personal data relating to the data subject is obtained indirectly from third-party sources or databases. In any case, the data subjects have the right to seek confirmation of the fact regarding the processing of their personal data by the data controllers and, upon such

[32]See Mahsa Shabani and Pascal Borry, "Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation, *European journal of human genetics* 26 (2018) 149.

[33]See Article 10 of the GDPR.

[34] See Article 4 (7-10) of the GDPR.

[35]For a comprehensive discussion on the related obligations that could provide a lawful basis for personal data processing see Oliver Butler, "Obligations Imposed on Private Parties by the GDPR and UK Data Protection Law: Blurring the Public-Private Divide" *European public law*, 24, no.3 (2018): 555.

[36] See Article 8 (2) of the GDPR.

[37]See Article 12 of the GDPR.

confirmation, to seek access to the personal data and various related information.

The GDPR recognises a range of other specific rights of the data subjects against the data controllers, including the right to seek rectification for any inaccuracies in their personal data, right to complete incomplete personal data, right to the erasure of personal data or right to be forgotten[38], the right to restrict the processing of their personal data, and right to data portability through the receipt of personal data from one controller and transmission to another[39]. Interestingly, the right to data portability confers upon the data subject the right to receive their personal data from the controller in a structured and commonly used machine-readable interoperable format[40]. This signifies its direct relevance to the digitalisation process, which also involves converting relevant information and data into a machine-readable digital format, as discussed earlier in this paper. Therefore, compliance with this obligation will be quite feasible for data controllers using digitalisation. Finally, the GDPR recognises a set of significant rights of data subjects, which have some serious implications upon personal data processing. The first right, namely the right to object to the very processing of personal data and related profiling, could impede any enterprises dealing with personal data. The second right in this regard has a specific implication for digitalisation, as it may potentially involve automated processing of personal data. The GDPR bestows the data subject with the right 'not to subject to a decision' made solely based on automated processing or profiling of personal data, which significantly affects or produces legal effects upon the data subject[41]. This right has the potential to limit the use of the digitalisation process in handling personal data.

Controllers and processors of personal data have distinct responsibilities and duties under the GDPR. Controllers have the responsibility to implement appropriate technical and organisational measures to ensure that data processing is carried out in compliance with the GDPR. They are also required to implement such technical and organisational measures designed to implement data-protection principles and to ensure that, by default, only the necessary personal data for specific processing needs are indeed processed. In addition, the GDPR mandates the integration of necessary safeguards into data processing. The design and implementation of relevant technical measures to ensure the default protection and the integration of necessary safeguards should be effectively made feasible. Controllers and their representatives have an obligation to maintain a record of all data processing activities that are under their responsibility and should make it available for a possible inspection by the 'supervisory authority' established by a member state under the GDPR[42]. The GDPR imposes a range of other important obligations upon the controller, which includes the notification obligation about any data breach to the supervisory authority of the relevant member state, obligation to document such breaches and promptly communicate with the affected data subject if the breach could result in a high-risk situation, obligation to carry out data impact assessment and to consult the supervisory authority in advance if the processing of personal data could result in a high-risk situation, etc.

Processors have specific responsibilities too. A processor should process personal data strictly in accordance with a specific set of stipulations that are to be included in a contract[43] or a legal act as per the prescription of the GDPR[44]. According to the GDPR, the contract or other legal act binding upon a processor should be governed by the law of the Union or a member state. A processor must refrain from engaging another processor without the controller's prior written authorisation. However, on behalf of the controller, when a data processor delegates the processing work to another processor, the GDPR mandates that the other processor should also be imposed with the same data protection obligations governing the controller and the original processor[45]. The GDPR also recognises that if a processor infringes the GDPR in certain circumstances, the processor will be considered as a controller with respect to the processing in question. As a result, the concerned processor would be required to undertake the obligations of a controller as prescribed by the GDPR. The potential processors in the context of digitalisation should be aware of this risk of being treated as a controller and the additional onus of compliance it may entail. Like the controllers, the processors and their representatives are also required to maintain the record of all data processing activities done on behalf of any controller and should furnish it to a supervisory authority in the event of its demand. Other notable obligations of the processors arising out of the GDPR includes the obligation to notify any personal data breach to the controller obligation not to process personal data in their access without instructions from the controller, etc.

The GDPR imposes certain obligations upon both the controller and the processor. They include the obligation to cooperate with the supervisory authority and make relevant records available, obligation to implement appropriate technical and organisational measures to provide suitable

[38] Cesare Bartoliniand and Lawrence Siry, "The right to be forgotten in the light of the consent of the data subject", *Computer law and security review* 32, no.2 (2016): 218

[39] Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, and Ignacio Sanchez, "The right to data portability in the GDPR: Towards user-centric interoperability of digital services" *Computer law and security review* 34, no.2 (2018): 193.

[40] See para 68 of the Preamble and Article 20 (1) of the GDPR.

[41] See Article 22 of the GDPR.

[42] Apart from supervisory authorities established by individual member states, the GDPR also recognizes the role of a European Data Protection Supervisor.

[43] The European Commission or any supervisory authority established by a member state under the GDPR may lay down or adopt relevant standard contractual clauses, which could be used in the contracts between a controller and a processor.

[44] The specific stipulations are prescribed under Article 28 (3) (a-h) of the GDPR. The prescription of the GDPR that such contracts or the other legal acts should be in writing recognizes electronic form to satisfy the requirement and such recognition is quite pertinent to digitalization.

[45] The specific purpose of such imposition is to ensure that appropriate technical and organizational measures could be guaranteed when an original processor delegates the task of personal data processing to another processor. In this context, the need to guarantee appropriate technical measures is particularly relevant in digitalization process.

security to the processing of personal data[46], obligation to designate a 'data protection officer' in prescribed circumstances and to secure the involvement of the officer in all issues related to personal data protection, obligation to comply with relevant conditions before transferring certain personal data to a third country or international organisation, etc. Finally, some obligations arising under the GDPR could be discharged either by the controller or the processor. For example, the controller or a processor could designate a representative in the Union in the circumstances when a controller or processor is not established in the Union but processes personal data of the data subjects in the Union.

To prevent any potential undermining of the GDPR standards in the context of cross-border personal data transfers, outside the territory of the EU or to international organisations, the GDPR mandates the controller and the processor of personal data to comply with the provisions of the GDPR strictly, including certain conditions specifically prescribed in this regard. The core conditions in this regard warrants transfer of personal data that are carried out subject to an 'adequacy decision' by the European Commission as well as ensuring that enough safeguards for data protection are in place. When there is already a standing decision by the Commission that a third country or the international organisation in question has an adequate level of protection, data transfer to them could be made without specific authorisation[47]. In the absence of an adequacy decision, such transfers could be made by a controller or processor only after ensuring that a prescribed set of safeguards are in place. Apart from such safeguards, the transfer is also subject to the blanket condition that enforceable rights and effective legal remedies are available for the data subjects whose personal data are to be transferred.

Two categories of prescribed safeguards exist. While the first category of safeguards could be provided without the authorisation of a Supervisory Authority, the second set of safeguards could only be provided with the authorisation of a relevant Supervisory Authority[48]. The safeguards, which may be provided without authorisation, includes those which derive from 'legally binding and enforceable instruments between public authorities' or from 'binding corporate rules' approved by a competent supervisory authority in accordance with the consistency standards recognised by the GDPR[49]. In contrast, some safeguards like those provided through certain types of contractual clauses require the authorisation of a competent Supervisory Authority. Although the GDPR has provided strong protection for cross border transfer of personal data, it recognises specific situations when such transfer could be made without an adequacy decision or appropriate safeguards[50]. The GDPR also requires the European Commission and supervisory authorities in the member states to promote international cooperation to achieve effective data protection in the context of cross-border transfer of personal data. As supervisory authorities in individual member states play a very important role in ensuring compliance, the GDPR provides detailed rules governing their establishment, constitution, competence, tasks, and powers. The GDPR prescribes cooperation between supervisory authorities and provides rules governing mutual legal assistance and joint operations among them. The GDPR also establishes a 'European Data Protection Board', consisting of the heads of one supervisory authority from each EU member state and the head of the European Data Protection Supervisor, to carry out a whole array of tasks aimed at promoting the consistent application of the GDPR[51].

If the data subjects perceive that the processing of their personal data infringes the GDPR, they have the right to complain to a relevant supervisory authority. The data subjects could seek a further judicial remedy against the decision of the supervisory authority. The judicial remedy could be sought even in cases where the supervisory authority does not act upon the complaint or fail to inform the progress or outcome within a specific period. Data subjects may decide to seek a judicial remedy against a controller or processor, who process their personal data without compliance with the GDPR. The data subjects could exercise these rights themselves or authorise certain prescribed non-profit bodies to exercise such rights on their behalf. This recognition of the possibility to be represented by NGOs and associations aimed at securing data protection rights enhances the possibility of initiating class action in instances where there are widespread infringements of the GDPR. Although the above proceedings are mainly recognised as the rights of the data subjects, the GDPR in prescribing the right to receive compensation recognises the entitlement of "any person" suffering damage (material or otherwise) because of the infringement of the GDPR. The liability is primarily imposed upon the controller, although a processor could become liable for non-compliance of the provisions of the GDPR specifically prescribed for them or for acting against or outside the scope of the lawful instructions given by the controller. Moreover, the infringement of the GDPR would also attract the imposition of administrative fines by the relevant supervisory authority. In addition, member states could prescribe other penalties for infringements, including for acts that are not subjected to administrative fines.

Finally, it is significant to note that despite providing a very strong protection of personal data, the GDPR recognises the need for achieving a balance *viz a viz* the exercise of other rights or other genuine needs for processing of personal

[46] Pseudonymization and encryption of personal data form an important part of such security measures. For an analysis of the relevant benefits of pseudonymization and anonymization see Mike Hintze and Khaled El Emam, "Comparing the benefits of pseudonymization and anonymization under the GDPR" *Journal of Data Protection and Privacy* 2, no.2 (2018): 145

[47] See Article 45(1) of the GDPR.

[48] See Article 46(2) and 46(3) of the GDPR.

[49] The binding corporate rules should have been approved by the Supervisory Authority in accordance with Article 63 of the GDPR and subject to the conditions prescribed by Article 47(1) (a-c). For an exposition of how business enterprises could utilize binding corporate rules to design a privacy program to implement the GDPR standards see John Bowman and Myriam Gufflet "Meeting the Challenge of a Global GDPR and BCR Programme" European data protection law review 3 (2017): 257

[50] See Article 49 (1) (a-g).

[51] See Articles 68 and 70 of the GDPR.

data. Therefore, the GDPR has provided a distinct set of provisions governing specific processing situations involving personal data. Specific provisions are prescribed governing the processing of personal data in the context of exercising the freedom of expression, right to information, right of public access to official documents, processing for the purpose of national identification, processing in an employment context, processing for certain purposes of archiving, processing in contexts involving obligations of secrecy and processing in situations involving data protection rules of churches and religious bodies. Entities engaged in digitalisation should pay specific attention to the special provisions governing the above specific situations and should accordingly adapt to the balanced approach.

IV. PERSONAL DATA PROTECTION IN MACAU SAR AND THE RELEVANCE OF THE GDPR

Macau SAR introduced its key legislation governing the processing and protection of personal data by virtue of Law 8/2005. As a special administrative region of the People's Republic of China, Macau enjoys legislative freedom to enact its own laws. By virtue of its historical connections with Europe, some of the domestic laws of Macau have distinct traits from the European legal tradition[52]. As Law 8/2005 has been characterised as the "most European influenced data privacy law in Asia"[53], it becomes relevant and necessary to comparatively assess the law with the new GDPR. Although a detailed and systematic comparison of the two instruments is beyond the scope of this paper, the remainder of this section will compare few features to identify whether future reforms in Macau law in lines with the GDPR is desirable.

The fundamental principle of Law 8/2005 mandates transparency and strict respect for the right to privacy as well as other fundamental rights and freedoms. The scope of application of this law extends primarily to the processing of personal data by automatic and manual means. It even applies to the processing of personal data in the context of public safety. It also applies to any video surveillance and other forms of capture by controllers, who are either domiciled or based in Macau or have made use of computer or network access providers established in Macau. However, the act does not apply to the processing carried out by a natural person in their personal or household activity unless it involves any systematic communication and dissemination. In comparison with the GDPR, the Macau law differs with respect to both the material and territorial scope of application. Regarding the material scope, the Macau law by default applies to the processing of personal data in the context of public safety subject to some exceptions, while the GDPR provides a blanket exclusion for such processing to address threats to public security. In terms of territorial scope, the Macau law is more limited in the context of video surveillance, whereas the GDPR has a much wider reach upon the acts of monitoring the behaviour of data subjects and offering goods and services to them from outside the Union.

The comparison of key definitions in the Macau law and the GDPR indicates that the number of definitions, as well as their scope, are much larger under the GDPR. The differences demonstrate that more efforts to expand the number and scope of the defined terms are inevitable in the future reforms of data protection law in Macau. About the prohibition of processing sensitive data under the Macau legislation, it does not contain the prohibition found in the GDPR relating to the processing of biometric data for identifying any natural person[54]. However, the absence of specific reference to biometric cannot be perceived as a limitation because the definition of 'personal data' in the Macau legislation is comprehensive to encompass 'information of any type relating to any identifiable natural person'. Biometric information will fall within the definition and consequently should enjoy the same level of protection any other types of explicit category of personal data would enjoy.

Apparent differences regarding the rights of data subjects recognised under the Macau legislation and the GDPR are visible. For example, the GDPR mandates 'transparency' in providing information to the data subjects regarding their personal data that are being processed. This is prescribed as one of the general standards governing different 'rights of the data subjects' before the scope of the 'right to information' of the data subject is specifically defined by the GDPR. In comparison, although the Macau law does not prescribe general standards governing various rights of the data subjects, the need for transparency in furnishing information to a data subject could be derived from the general principle governing the whole legislation. It is evident from the general principle enshrined at the very outset of Law 8/2005 that the law mandates all processing of personal data should be carried out in a transparent manner. By virtue of this general principle, any data subject could demand transparency regarding their personal data processing while exercising their right to information. However, as referred to earlier, the scope of the right to information as enshrined in the GDPR is much wider than the one recognised under the Macau legislation. For example, the right in the GDPR comprehends information pertaining to the adequacy decision and safeguards relating to the transfer of personal data to a third country or international organisation, the details of the data protection officer, etc., which are not present in the Macau legislation. The right to information of the data subjects in two distinct contexts, namely when the personal data have been obtained from the data subject and when the same has been obtained from sources other than the data subject, has a much wider scope in the GDPR in comparison with the Macau legislation[55].

The right to access granted to the data subjects also differ between the GDPR and Macau legislation. While the basic elements of the right remain similar, there are some striking

[52] The data protection law of Macau is also found to have the European influence see Graham Greenleaf, "The influence of European data privacy standards outside Europe: implications for globalization of Convention", *International data privacy law* 2, no. 2 (2012): 68

[53] See Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives*, (Oxford, UK: Oxford University Press, 2015), 267.

[54] See Article of Law 8/2005 of MSAR and Article 9 of the GDPR.

[55] Compare Article 13 and 14 of the GDPR with Article 10 of Law 8/2005.

differences. Firstly, certain information to which the right of access is recognised, namely the information regarding the implemented safeguard measures, while transferring data to a third country or an international organisation, etc., is only present in the GDPR. Secondly, certain provisions explicitly restricting the right of access of the data subjects[56] or providing access rights only through another person[57] seems distinct in the Macau legislation. Although other similarities and differences could be seen in a comparison of the remaining provisions of the Macau legislation with the GDPR, it is evident that there is certainly a need to review the Macau law in the light of the new standards introduced by the GDPR. This is crucial, not just to sustain the characteristic that Macau protects personal data in par with high European standards but also to ensure that Macau data protection regime constantly evolves to shield the personal data privacy of its people effectively from increased threats emanating from digital sources within and outside its territory.

V. CONCLUSION

The close analysis of the key legal standards governing the protection of personal data in Europe reveals its potential as an inevitable source of reference for any jurisdiction seeking to enact or enhance their domestic legal regimes governing personal data protection. However, the question as to whether the European standards could serve as a potential source of legal transplants would depend on various factors, including the domestic conditions, regional cooperation needs, and international legal obligations of specific jurisdiction in question. From the systematic analysis in this paper, it can be concluded that European legal standards have a very strong potential to serve as a source of legal transplants for any jurisdiction—several factors identified in this paper support such a conclusion. Firstly, Europe has been the pioneer in legally protecting the privacy and personal data among several regions in the world. Since the 1950's when the general right to privacy was sought to be protected by the European Convention, Europe has always been the pioneer in the specific normative development governing personal data protection.

The analysis of the COE Convention in this paper revealed some of its intriguing set of obligations that were well ahead of its time in seeking to protect personal data in the circumstances of automated processing of data. It is not just the pioneering nature of these standards but the efforts made for the constant transformation of the related standards to meet the needs of personal data protection in an environment dictated by the unprecedented evolution of information technology. Major landmark instruments examined in this paper evidences a conscious effort to ensure that the legal standards keep in phase with the technological evolution. The balancing nature of the objectives of such instruments is also a key for its utilitarian as a source of legal transplant. Despite the primary emphasis on human rights protection, right to privacy and personal data protection, the analysis in this paper reveals that the aim was not limited to that protection but to ensure free flow of data between member states to support other interests of the society, including economic goals. Such a fine balance sought to be achieved by the European legal standards governing the protection of personal data should serve as one of the important factors to reinforce its candidacy as a source of legal transplant.

In addition, the development of a systematic legal framework governing different stages or categories of issues (arising in a context of personal data collection to the processing as identified earlier in the analysis of the EU Directive 1995) would enable other jurisdictions to segment the related legal norms and determine which of the relevant set of norms would be the suitable for transplant based on their respective domestic needs. The systematic framework, which is also evident in the most recent instrument of GDPR, does not impose the need to transplant the whole regime but provides much-needed flexibility to selectively adopt pertinent norms. The specificity of the protection of personal data in response to the needs of the modern times and technological environment as revealed in the analysis of the instruments promulgated in the early years of the 21st century, namely the European Charter of Fundamental Rights 2000 as well as the EU Privacy and Electronic CommunicationDirective 2002, demonstrates that European normative standards could serve as the most vibrant and modern source for legal transplant. In addition, the reliability of the relevant European legislative instruments serving as a source of legal transplants is substantially strong given the stringent judicial scrutiny to which they are subjected. The grounds of nullification of the 2006 European Data Retention Directive by the European Court of Justice, as discussed earlier in the paper, is a good example of the objectivity of the European legal standards making them quite suitable for transplantation.

The determined effort to introduce a comprehensive regulatory regime of the GDPR, based on the experiences gained from several decades of legal efforts to protect personal data, is a major milestone that enhances the potential of the GDPR to become the most influential source for domestic legal developments in personal data protection in various jurisdictions around the world. The vitality of the GDPR to serve as an instrument of regulation of personal data protection both in a domestic as well as in a cross-border context makes it a more desirable source of transplant. In addition, various inherent characteristics of the GDPR, asrevealed in the detailed analysis of the instrument in this paper, demonstrate its desirability for diverse conditions facing various stakeholders in any personal data processing situation. For example, regarding the legal safeguards imposed upon any transfer of personal data to jurisdictionsoutside the EU, the need to ensure the availability of equal protection standards should motivate many jurisdictions to emulate the GDPR standards. Although this could make the GDPR a key source of legal transplant, especially those jurisdictions that have close European ties in their economic relations, its desirability is not driven only because of the prescription of equal protection standards.

[56]See Article 11 (6) of Law 8/2005.
[57]See Article 11(5) of Law 8/2005.

It is important to note that the recognition under the GDPR enabling data transfers based on other alternative protection, namely standard forms of contracts or binding corporate rules etc., makes it a desirable model. As these alternative safeguards are based on private contractual or corporate initiatives rather than the public legislative process in a foreign jurisdiction, the GDPR model should be equally appealing to a wider number of jurisdictions.Especially, given the successful legal challenges against public agreements like the Safe Harbour Agreement and Privacy Shield between the EU and the US, recognition of the private arrangements to serve as the necessary safeguards for data transfer is a fundamental feature of the GDPR to ensure smooth economic relations between private parties This should make the GDPR an inevitable source for consideration in any legal transplant project.

Finally, based on the above findings, as well as from the past legislative experience in the Macau SAR, it is easy to conclude the relevance of the GDPR serving as an essential source of reference for future development of personal data protection standards in the SAR. However, it is relevant to bear in mind several caveats related to this process. First, regarding the past legislative experience of personal data protection in the Macau SAR, the substantial influence of the EU Data Protection Directive of 1995 should be seen in the context of the early years of the establishment of the SAR, when the nature of its economy and international economic relations were not the same as it is currently or will be in the future. For example, at present, the SAR is in the course of increasing regional economic integration like the Greater Bay Area cooperation southern China and Hong Kong SAR. It is also destined to play a strategic role as a platform to promote economic relations of the PRC with other Portuguese speaking countries (PRC-Lusophone cooperation). It is also increasingly called upon to partake in the opportunities provided by the Belt and Road Initiative of the PRC. In addition, its trade and investment liberalisation with the PRC has been substantially consolidated by the series of Closer Economic Partnership Arrangements (CEPA) and supplements. Therefore, any future modernisation of the SAR's personal data protection regime should also be regionally focused, seeking to harmonise with the data protection legal standards of the PRC, which has increasingly been focused on domestic legal reforms governing data protection in recent years.

Moreover, Macau SAR's economic transactions with Hong Kong have increased considerably in comparison with the early years of its establishment. Although in the past, Hong Kong was under the administration of the United Kingdom that was a member of the EU, its domestic data protection legal standards have notable differences with the English law and the provisions of the GDPR. Therefore, the consideration of the legal characteristics of the Hong Kong personal data privacy regime and exploring the need for any harmonisation with the same should also be of relevant consideration for the Macau SAR. Finally, with the expansion of its gaming and tourism industry and its plans to diversify the economy in the future, Macau should also pay sufficient attention to the other international developments in data protection legal standards and should give due consideration to them. Therefore, in the light of the above findings, it is concluded that the Macau SAR,in its future legal reforms to personal data protection,should seek for a comparative reference of the personal data protection standards involving the European legal standards, the legal standards in the PRC and Hong Kong as well as other key international standards of relevance, instead of using a single source of legal transplant.