ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

DOTTORATO DI RICERCA IN

DIRITTO EUROPEO

Ciclo XXXVI

Settore Concorsuale: 12/E2- Diritto Comparato

Settore Scientifico Disciplinare: IUS/02-Diritto Privato Comparato

The Protection of Personal Data of *Netizens* in International, EU, and Chinese Legal Frameworks

Presentata da: Dongshu Zhou

Coordinatore Dottorato

Prof. Pietro Manzini

Supervisore

Prof.ssa Angela Carpi

Co-Supervisore

Prof.ssa Marina Timoteo

Esame finale anno 2024

FUNDING ACKNOWLEDGE

I am extremely honored and grateful to the China Scholarship Council (CSC) for awarding me a full scholarship that covers all three years of my PhD program in EU Law.

This generous support has not only alleviated the financial burden of my education but has also allowed me to focus wholeheartedly on my research and academic pursuits. The CSC's commitment to fostering international education and research collaboration has been pivotal in shaping my academic journey. I extend my heartfelt thanks to the CSC for this incredible opportunity, which will undoubtedly contribute to my growth and development as a scholar in the field of law.

本论文成果得到国家留学基金资助

ABSTRACT

Nella società contemporanea, l'importanza di Internet è equiparabile all'aria che respiriamo. Nonostante spesso si percepisca la rete come un luogo privato, ogni interazione su Internet lascia tracce, che si traducono in dati archiviati dal sistema. Questi dati, sia personali che non, giocano un ruolo cruciale nella nostra vita quotidiana e sono spesso definiti dagli studiosi come il nuovo "petrolio" del secolo.

La presente tesi dottorale si propone di esplorare come gli strumenti giuridici internazionali, europei e cinesi regolamentino il diritto alla protezione dei dati personali dei "*Netizens*", in quanto l'Internet, oggi, è la principale fonte di raccolta e trattamento dei dati personali, ma è anche il terreno fertile per attività illecite. La mancanza di confini fisici in questo ambiente virtuale complica il compito dei legislatori nel formulare norme funzionali ed efficaci per la protezione dei dati personali.

Attraverso una comparazione approfondita delle normative, includendo fonti giuridiche, dottrina, giurisprudenza e principi vigenti, il lavoro si propone di analizzare se vi sia una reciproca influenza tra gli strumenti normativi presi in esame. Tale analisi è motivata dalla necessità di garantire che il diritto alla protezione dei dati personali, per essere efficace, sia garantito a livello internazionale, in modo uniforme. In aggiunta, è l'interessante svolgere l'analisi comparativa fra gli ordinamenti dell'Unione Europea (UE) e cinese in quanto la legislazione europea ha assunto un ruolo di primaria importanza nel panorama normativo internazionale, grazie al suo Regolamento Generale sulla Protezione dei Dati (RGPD o GDPR), ufficialmente regolamento n. 2016/679 e ha influenzato l'ordinamento internazionale in materia di protezione dei dati personali, mentre la Cina, nonostante il suo giovane sistema legislativo, detiene il mercato digitale più vasto al mondo. Si tiene, inoltre, in considerazione il rapporto fra la protezione dei dati personali e la recente sfida derivante dall'intelligenza artificiale.

Il lavoro è strutturato in cinque parti. La prima parte esamina le fonti giuridiche relative alla protezione dei dati personali dei *Netizens*; la seconda parte analizza il concetto di dati personali nell'ordinamento internazionale e dell'UE, nonché il concetto di informazioni personali nella legislazione cinese; la terza parte si focalizza sulle regole del consenso dell'interessato per il trattamento dei dati personali; la quarta parte esplora i diritti riservati all'interessato nei tre ordinamenti, mentre l'ultima parte delinea le regole per il trasferimento transfrontaliero dei dati e le sanzioni previste in caso di violazione delle norme sul trattamento dei dati.

TABLE OF CONTENTS

INTRODUCTION

In the era marked by the relentless march of technology and the seamless interconnectivity of our digital world, the subject of personal data protection has risen to the forefront as a paramount concern for individuals, organisations, and governments across the globe. The rapid expansion of the digital landscape has brought with it a host of intricate legal challenges, none more pressing than the imperative to safeguard personal data on an international scale. Moreover, personal data has come to be often compared to the new “oil” of the twenty-first century, signifying its immense value and importance.

While the significance of personal data protection may seem self-evident, it is essential to recognize that not all countries acknowledge the right to personal data protection as an independent and autonomous right.

In the context of the international legal framework, the right to personal data protection is often viewed as a subsidiary aspect of the broader right to individual privacy, thereby not being recognized as a standalone right. In the international context, a breach of personal data protection is equated with a violation of an individual's right to privacy. Although a similar perspective was once shared by both the European Union (EU) and China, these two distinct legal systems now acknowledge the right to privacy and the right to personal data protection as two separate and integral rights.

This study aims to undertake a comprehensive exploration of personal data protection as it pertains to netizens within three distinct legal systems: international law, EU, and China.

The term “netizen” means a portmanteau of “internet” and “citizen”, which designates individuals who actively and meaningfully engage in the online community and the internet. Netizens participate in a wide array of online activities, including social media interactions, blogging, forum discussions, and various other forms of digital communication. These individuals contribute by expressing their opinions,

sharing information, and engaging in discussions and interactions with others on the Internet. The concept of “netizens” is particularly pervasive in China, where people view themselves as integral to the online world, actively shaping the culture and discourse of the internet.

The online realm, in its boundless nature, transcends borders, thereby instigating a heightened interest in providing a comparative perspective within this domain.

This research undertakes the task of comparing the legal frameworks for personal data protection within the international, EU, and Chinese legal systems for several compelling reasons. First, it endeavors to unravel how these distinct legal systems have influenced the development of personal data protection instruments. Second, the EU and China stand as significant global partners. Third, the EU possesses a well-established and mature legal framework for personal data protection, while China, as one of the world's most populous nations, has only recently enacted its first comprehensive law for personal information protection, known as the Personal Information Protection Law (PIPL), which came into effect in November 2021.

For instance, the present legal standards for personal data protection within the EU are commonly categorised as the “third generation”.

This classification derives from the fact that the first generation included OECD Governing the Protection of Privacy and Transborder Flows of Personal Data adopted in 1980, as well as Convention 108, adopted in 1981, by the Council of Europe. The second generation featured the Data Protection Directive (DPD) in 1995, while the current third generation is represented by the General Data Protection Regulation (GDPR) implemented in 2016.

The GDPR, a landmark regulation, achieved maximum harmonisation when it came into effect on May 25, 2018, supplanting the prior Data Protection Directive. A central focus of the GDPR is to ensure that data subjects are adequately informed, enabling them to make informed decisions regarding how data controllers manage their data.

Convention 108, enacted by the Council of Europe, underscores the contribution of international organisations to the development of personal data protection. It is significant to note that, until 1995, the EU did not possess its legal instruments for personal data protection. In stark contrast, the Chinese PIPL, in effect since November 2021, is viewed as both the "third generation" by the EU in comparison to the GDPR, while China considers it the "first generation" of personal data/information protection legislation by the China side.

Part one of this thesis embarks on an analysis of the legal instruments governing personal data protection within the international, EU, and Chinese legal systems.

Chinese legislators have chosen the term "personal information" instead of "personal data" employed by international and EU legal systems. This divergence prompts a dedicated examination in part two of this thesis to determine if these terms are synonymous or if notable distinctions exist between them.

A universal aspect of all legal instruments governing personal data protection is the requirement of the consent of the data subject before handling personal data. Consent represents the legal basis for processing personal data. Part three of this thesis delves into the commonalities and diversities in provisions relating to the consent of the data subject within international, EU, and Chinese legal systems.

Another pivotal component of this study concerns the rights of the data subject and is discussed in part four of this thesis.

Finally, the regulation of the transfer of personal data and the corresponding sanctions in cases of infringements of personal data protection rules within international, EU, and Chinese legal frameworks will be explored in detail.

In summary, this thesis embarks on a multifaceted exploration of personal data protection within the international, EU, and Chinese legal systems, spanning various aspects, including terminology, the consent of data subjects, data subject rights, and enforcement measures. Through this comprehensive analysis, it aims to shed light on the evolving landscape of personal data protection in an interconnected digital world and its significance in safeguarding the rights and privacy of individuals across borders.

PART 1
SOURCES OF PERSONAL DATA (INFORMATION) PROTECTION LAW

Personal data protection has become increasingly important in our society due to advanced technological development. The number of cases of personal data breaches has increased significantly in the last decade, often in connection with the use of technology. Although personal data protection has been a topic of great importance and social attention in this last decade, the legislation for its protection of personal data was in place much earlier than expected.

In the international legal order, the process of personal data protection began forty years ago. In 1980, the Organisation for Economic Cooperation and Development (OECD) adopted guidelines that regulated the protection of privacy and personal data, representing the first non-binding international legal standard on the matter. The following year, in 1981, the Council of Europe approved Convention 108, which entered into force in 1985. Convention 108 is the only international legally binding instrument on the protection of privacy and personal data.

At this juncture, it is necessary to emphasize that neither of these legal instruments recognises the right to personal data protection as an individual and distinct right. According to these two legal instruments, the right to personal data protection is recognised as a sub-right under the right to privacy. Indeed, the purpose of enacting these legal instruments is only to protect individual privacy.[1]

---

[1] Council of Europe Treaty Series, No. 223 of Council of Europe, *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, of 10 October 2018; and *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, of 128th Session of the Committee of Ministers, of 18 May 2018, Preamble.

Lawmakers did not consider it necessary to distinguish between the right to privacy and the right to the protection of personal data, since cases of personal data breaches were less prevalent than today, owing to the risk of personal data disclosure being connected to technological development. Forty years ago, there were no personal computers, no internet, no social networks, and most of the population had no contact with computers; therefore, the need to protect personal data was less, and the importance of protecting privacy was greater. For this reason, lawmakers affirmed the need to evaluate cases of a personal data breach using the so-called privacy approach.[2]

Even though the current social context is vastly different from forty years ago, the lawmakers of the international legal order have not deemed it necessary to convert the right to the protection of personal data into an individual right. The OECD Privacy Guidelines and Convention 108 have been subject to revisions in the last decade. Yet, the need to separate the rights of privacy and personal data protection has not been mentioned in any revision working papers. Therefore, even today, the right to personal data protection in the international legal order remains a sub-right of the right to privacy.

The situation is different in the context of the European Union's (EU) legal order. The EU law makes a clear distinction between the right to privacy and the right to personal data protection.[3] The Charter of Fundamental Rights of the European Union (EU CFR) states that the right to privacy and the right to personal data protection are two separate constitutional rights.[4]

To prevent new risks arising from the advancement of new information technologies, the personal data protection legal instruments of the EU have evolved twice. The current primary EU legal instrument on personal data protection is the General Data Protection Regulation (GDPR), which is referred to as third-generation

[2] See, Part 2, Chapter 4, Paragraph 1.

[3] See, Streinz, *The Evolution of European Data Law*, p.p. 910-913.

[4] Charter of Fundamental Rights of the European Union, O.J.E.C. C 364/1, of 18 December 2000, Articles 7 and 8.

legislation by legal scholars.[5] The first generation was composed of Convention 108, and the second generation was the Data Protection Directive (DPD).

Nowadays, the right to personal data protection must be interpreted broadly, as personal data is used in several sectors, such as the artificial intelligence sector, which is an industry based solely on the use of data, and thus, personal data is inevitably also utilized.

Legal scholars have underscored that current international and EU legal instruments on personal data protection are considered inadequate, as they are too outdated for the current economic and social context.[6] According to Focarelli, in general, the legal standards of personal data protection have four deficiencies. Firstly, the legal standards on personal data protection should be global rather than regional. Secondly, most international legal standards do not represent binding legal instruments. Thirdly, the binding legal instrument, such as Convention 108, does not have adequate legal control, meaning no supervisory body has been set up in the rules adopted in the international legal order. Finally, the current personal data protection legal standards are not able to promote the current economic needs, due to the legal standards being too protective of data subjects.[7]

This Part describes the sources of personal data protection, which form the necessary basis for studying the matter. Additionally, a comparison between them is provided. Furthermore, the EU proposal on Artificial Intelligence (AI Act) is analysed, as it will have a significant impact when it comes into force for the protection of the personal data of netizens.

---

[5] D. Erdos, *European Data Protection Regulation, Journalism, and Traditional Publishers*, Oxford University Press, 2019, p.p. 151-152; and S. Gutwirth, Y. Poullet, and P. De Hert, *Data Protection in a Profiled World*, Springer, 2016, p.p. 3-30.

[6] C. Focarelli, *La privacy. Proteggere i dati personali oggi*, Il Mulino, 2015; A. M. Froomkin, *The Death of Privacy?*, Stanford Law Review, vol. 52, 2000; and S. Garfinkel, *Database Nation: The Death of Privacy in the 21st Century*, O'Reilly Media, 2001.

[7] See, Focarelli, *La privacy. Proteggere i dati personali oggi*, p.p 105-106.

The Part is divided into three Chapters. The first states the sources of personal data protection law under international legal instruments; the second explains the sources of personal data protection law under EU legal instruments; and the third Chapter analyzes the sources of personal information protection law under the Chinese legal system. The Part also deals with the previous generations of sources of personal data protection law and the relevant principles and guidelines adopted by international organizations in this matter. These are not a source of law and are not binding legal instruments, but they are the main recommendations that can influence the formation of legal standards in this matter. The Part will end with a comparative view of the sources of personal data (information) protection law, exploring the existing relationships between the legal standards, studying their reciprocal influences, and analysing common and divergent principles, regardless of whether they have influenced their formation or not. Particular attention will be paid to the role of international and European legal standards of personal data protection law with Chinese personal information protection law, due to the latter law coming into force in 2022.

Chapter 1
The International Sources of Personal Data Protection Law

International organisations have developed various legal instruments for the protection of personal data, some of which are binding and some of which are not. These include the 1980 Privacy Guidelines of the Organisation for Economic Co-operation and Development (OECD), the Convention 108 of the Council of Europe, Guidelines for the Regulation of Computerized Personal Data Files of the United Nations, the Privacy Framework of the Asia-Pacific Economic Cooperation (APEC), none of which, however, recognise the right to the protection of personal data as an individual and distinct right.

At this point, it should be noted, that according to the international legal order, the violation of personal data should be considered a violation of the right to privacy, since the international legal instruments recognise the right to the protection of personal data as a sub-right of the right to privacy. Therefore, the so-called "privacy approach" applies in international law.[8]

1. *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data of the OECD*

In 1980, the OECD adopted the Guidelines for the Protection of Privacy and Transborder Flows of Personal Data, also known as the 1980 OECD Guidelines; or, more commonly, the OECD Privacy Guidelines.[9] The Guidelines were amend-

[8] See, Part 2, Chapter 4, Paragraph 1.

[9] Organisation for Economic Cooperation and Development (also known as OECD*), Guidelines governing the Protection of Privacy and Transsnborder Flows of Personal Data*, on 23 September 1980.

ed in 2013.[10] Both the original version of the 1980 Guidelines and the revised version are non-binding legal instruments.[11]

In 2007, before the revision of the OECD Privacy Guidelines, the OECD adopted the Recommendation on Cross-Border Cooperation in the Enforcement of Laws Protecting Privacy,[12] which proposes to establish a framework for enforcement cooperation and to promote cross-border cooperation on privacy laws through bilateral or multilateral enforcement agreements or memoranda of understanding (MOU).[13] As a result of this recommendation, there are many success stories of bilateral cooperation in cross-border and multilateral cooperation to report. For example, the Dutch Data Protection Authority (DPA) worked with the Portuguese DPA to get the university to block access to the website. Another example is that the DPAs in Canada, France, Germany, Israel, Italy, Ireland, the Netherlands, New Zealand, Spain, and the United Kingdom issued a joint letter to a company in April 2010 to point out the importance of adequately considering data protection aspects before launching new services.[14]

The 2013 version introduced a privacy management program, personal data security breach notifications, [15] and national privacy enforcement authorities.[16]

---

[10] Organisation for Economic Cooperation and Development (OECD), *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)*, C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79.

[11] Organisation for Economic Cooperation and Development (OECD), *Original Explanatory Memorandum to the OECD Privacy Guidelines (1980), in The OECD Privacy Framework*, OECD Publishing, 2013, p. 46.

[12] Organisation for Economic Cooperation and Development (OECD), *Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, C(2007)67/FINAL, 2007.

[13] Organisation for Economic Cooperation and Development (OECD), *Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD Digital Economy Papers, No. 178, OECD Publishing, 2011.

[14] Ibid, p.p. 11-14.

[15] See, OECD Privacy Guidelines, 2013, Paragraph 15.

[16] Ibid., Paragraph 19.

The OECD Privacy Guidelines represent the first international instrument regarding privacy and transborder flows of personal data and are composed of six parts. The first part describes general information and affirms that these Guidelines apply to personal data, whether in the public or private sectors.

The second part affirms eight basic principles: the collection limitation principle,[17] the data quality principle,[18] the purpose specification principle,[19] the use limitation principle,[20] the security safeguards principle,[21] the openness principle,[22] the individual participation principle,[23]and the accountability principle.[24] These principles are reflected worldwide in all relevant personal data protection frame-

[17] There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

[18] Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up to date.

[19] The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

[20] Personal data should not be disclosed.

[21] Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification, or disclosure of data.

[22] There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

[23] An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

[24] A data controller should be accountable for complying with measures which give effect to the principles stated above.

works, including the EU personal data protection law.[25] It is said that the OECD Privacy Guidelines have influenced the personal data protection law of the OECD member states.[26] The third part states implementing accountability. The fourth part regards free flow and legitimate restrictions under international applications. The fifth part focuses on national implementation. The last part underlines the importance of international cooperation and interoperability.

2. *Convention for the Protection of Individuals regarding Automatic Processing of Personal Data of the Council of Europe (Convention 108)*

In 1981, the first and currently only legally binding international instrument for the protection of personal data was adopted, the Convention for the Protection of Individuals regarding Automatic Processing of Personal Data, which was adopted by the Council of Europe on 28 January 1981 and entered into force in 1985.[27] This Convention is commonly referred to as Convention 108,[28] and was amended in 2018, also known as the "Modernised Convention 108" or "Convention 108+".[29] In this work, Convention 108 also refers to Convention 108+, the distinction should be made only when necessary.

---

[25] M. Kuschewsky, *The new privacy guidelines of the OECD: what changes for businesses?*, Journal of European Competition Law & Practice, Vol. 5, No. 3, 2014.

[26] See Focarelli, *La privacy. Proteggere i dati personali oggi*, p. 107.

[27] The Council of Europe is an international organisation born after the Second World War to unite the states of Europe to promote the rule of law democracy, human rights, and social development. Currently, the Council of Europe has 46 member states, 27 of which are EU member states.

[28] Council of Europe, European Treaty Series, No. 108, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, of 28 January 1981.

[29] Council of Europe, Treaty Series, No. 223 of Council of Europe, *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, of 10 October 2018; and *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, of 128th Session of the Committee of Ministers, of 18 May 2018.

Convention 108 was born to protect the right to privacy of an individual during their data processing, as the Convention recognises the right to privacy as one of the fundamental human rights.[30]

According to international standards for the protection of personal data, the right to the protection of personal data is not recognised as an individual and autonomous right but is considered a sub-right of the right to privacy.[31] This model of sub-right is now considered outdated, as legal scholars affirm that the right to privacy and the right to personal data protection are defined as twins and thus are not the same right.[32]

The European Court of Human Rights (ECtHR or ECHR, also known as the Strasbourg Court) can only apply Convention 108 based on Article 8 of the European Convention on Human Rights, which affirms the right to respect for private and family life, home, and correspondence,[33] since the right to the protection of personal data is not an individual and autonomous right under the European Convention on Human Rights (ECHR).[34] For this reason, Convention 108 does not, in principle, fall within the jurisdiction of the Strasbourg Court.[35]

---

[30] See, Convention 108, Preamble and Art. 1.

[31] See, Part 2, Chapter 4, Paragraph 1.

[32] P. De Hert and E. Schreuders, *The Relevance of Convention 108*, in European Conference on Data Protection on Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data: present and future, 2001, pp.63-76.

[33] See, Judgment of the ECtHR, of Grand Chamber, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, no. 931/13, of 27 June 2017; Judgment of the ECtHR, *Z v. Finland*, of 25 February 1997.

[34] Council of Europe, European Court of Human Rights, *Guide to the Case-Law of the European Court of Human Rights-Data protection*, 2021.

[35] Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights, *Handbook on European data protection law: 2018 edition*, Publications Office, 2019, page 25

The Convention applies to both the public and private sectors.[36] It protects individuals from personal data breaches and seeks to regulate the transborder flows of personal data. Today, 55 states have ratified Convention 108 into their legal systems, including 46 Council of Europe member states and 9 non-Council of Europe member states.[37] This means that all EU member states have ratified the Convention.[38]

Convention 108 is binding only on states that have ratified it and provides for the possibility of accession by states that are not members of the Council of Europe or international organizations.[39] Although Convention 108 allows non-members of the Council of Europe to accede, it remains a regional convention,[40] as its binding force is weakened for non-members of the Council of Europe,[41] since non-members of the Council of Europe, unlike members of the Council of Europe, are not obliged to accede to the European Court of Human Rights (ECtHR). From this point of view, there would be too many inequalities in the enforcement of Convention 108 between members of the Council of Europe members and non-members of the Council of Europe.[42]

Before the modernisation of Convention 108 in 2001, the Council of Europe adopted an Additional Protocol to Convention 108, entitled "Additional Protocol to the Convention for the Protection of Individuals concerning Automatic Processing of Personal Data regarding Supervisory Authorities and Transborder Data

---

[36] See, Convention 108, Article 3.

[37] The 9 no member states of the Council of Europe have ratified Convention 108 are: Argentina, Burkina Faso, Cape Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, Uruguay.

[38] S. Kwasny, A. Mantelero, and S. Stalla Bourdillon, *The role of the Council of Europe on the 40th anniversary of Convention 108*, Computer Law & Security Review, no. 40, 2021.

[39] See, Convention 108, Article 27.

[40] C. Kuner, *An international legal framework for data protection: Issues and prospects*, Computer Law & Security Review, 2009, pages 307-317.

[41] Ibid., page 313.

[42] C. De Terwangne, *Council of Europe convention 108+: A modernized international treaty for the protection of personal data*, Computer Law & Security Review, no. 40, 2021.

Flows".[43] Currently, only 44 of the 55 countries that have ratified Convention 108 have also ratified the Additional Protocol,[44] and 7 countries have signed the Additional Protocol but have not yet completed the ratification process.[45]

The Additional Protocol was heavily influenced by the EU DPD, as it establishes an independent data protection authority, restricts the flow of personal data, and introduces the right of appeal to the courts. This brings the standards of Convention 108 to a level comparable to that of the EU DPD,[46] demonstrating how an EU directive has impacted an international legal instrument.[47]

The principles introduced by the OECD Privacy Guidelines are all reflected in Convention 108 under Article 5.[48] Therefore, Convention 108 has taken over and developed the OECD principles, with the only difference being that the Council of Europe has them incorporated into a legally binding treaty.[49]

---

[43] Council of Europe, European Treaty Series No. 181, *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*, of 8 November 2001.

[44] The 44 countries that have ratified the Additional Protocol are Albania, Andorra, Armenia, Austria, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Hungary, Ireland, Latvia, Liechtenstein, Lithuania, Luxembourg, Monaco, Montenegro, Netherlands, North Macedonia, Poland, Portugal, Republic of Moldova, Romania, Serbia, Slovak Republic, Spain, Sweden, Switzerland, Turkey, Ukraine, Argentina, Cape Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, Uruguay.

[45] The 7 countries that have signed the Additional Protocol but had not gone through the ratification process are Belgium, Greece, Iceland, Italy, Norway, United Kingdom, Russian Federation.

[46] Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J.E.C. L 281/31, of 23 November 1995.

[47] L. A. Bygrave, *Privacy and Data Protection in an International Perspective*, Scandinavian Studies in Law, 2010, p. 187.

[48] G. Greenleaf, *The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108*, International Data Privacy Law, Volume 2, Issue 2, 2012.

[49] See, Focarelli, *La privacy. Proteggere i dati personali oggi*, p. 110.

Principles under Convention 108+ are the lawfulness principle, the fairness principle, the transparency principle, the purpose limitation principle, the data minimization principle, the data accuracy principle, the storage limitation principle, the data security principle, and the accountability principle. The lawfulness principle means that all personal data processing must be done lawfully. Lawful processing requires the consent of the data subject.[50] The fairness principle states that personal data processing must be processed fairly, meaning that controllers should notify data subjects that they will process personal data lawfully and transparently.[51] The transparency principle indicates that controllers must inform data subjects about their data use.[52] The purpose limitation principle stipulates that the processing of personal data must be done for a specific and well-defined purpose.[53] The data minimisation principle suggests that personal data processing must be adequate, relevant, and not excessive for the purposes for which it is processed.[54] The data accuracy principle states that the data controller must use accurate and up-to-date information.[55] The storage limitation principle states that the data controller must erase or anonymise data when it is no longer necessary for the data being processed.[56] The data security principle connotes that the data controller must have appropriate organizational measures in place to protect data against accidental, unauthorised, or unlawful access, use, modification, disclosure, loss, destruction, or damage.[57] The accountability principle denotes that the data controller is responsible for the processing of personal data.[58]

---

[50] See, Modernised Convention 108, Art. 5, Paragraph 3.

[51] Ibid., Art. 5, Paragraph 4, lett. a.

[52] Ibid., Art. 5, Paragraph 4, lett. a, and Art. 8.

[53] Ibid., Art. 5, Paragraph 4, lett. b.

[54] Ibid., Art. 5, Paragraph 4, lett. c.

[55] Ibid., Art. 5, Paragraph 4, lett. d.

[56] Ibid., Art. 5, Paragraph 4, lett. e.

[57] Ibid., Art. 7.

[58] Ibid., Art. 10, Paragraph 1.

Convention 108+ reinforces the principles of proportionality and data minimisation, the lawfulness of processing, transparency of data processing, and accountability of the data controller. It also extends sensitive data types, thus providing a more protective regime for sensitive data. It also introduces new rights for individuals in an algorithmic decision-making environment and requires the enforcement of "privacy by design". It can be said that, compared to Convention 108, Convention 108+ is more suitable for the current context.[59]

3. United Nations Resolution 45/95 of 14 December 1990

United Nations General Assembly Resolution 45/95 of 14 December 1990 adopted guidelines for the regulation of computerized personal data files.[60] The guidelines established six principles for computerized personal data files, namely the principles of lawfulness and fairness, the principle of accuracy, the principle of purpose-specification, the principle of interested-person access, the principle of non-discrimination, and the principle of security. These principles are not binding, and the same Resolution 45/95 states that these guidelines are only a guide for States.

The principle of lawfulness and fairness states that personal data must be collected or processed fairly and lawfully and in compliance with the principles of the Charter of the United Nations.[61] In addition, the principle of accuracy emphasises that whoever keeps personal data is responsible for compiling the files, and should regularly verify the accuracy and relevance of the data to avoid errors of omission, and that the data are regularly updated.[62] The principle of purpose specification

---

[59] See, Terwangne, *Council of Europe convention 108+: A modernized international treaty for the protection of personal data*, p.p. 1-12.

[60] UN General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*, 14 December 1990

[61] Ibid., point 1.

[62] Ibid., point 2.

states that the collection and processing of the data should be specified, and lawful and that the data subject should know this.[63] Moreover, the principle of interested-person access implies that the data subject has the right to know whether or not data concerning being is processed, to receive it in an intelligible form, and without unjustified delay or expense, and in the event of unlawful, unnecessary, or inaccurate entries, to obtain the relevant rectifications or erasures and, in the event of notification, to be informed of the recipients of the data.[64] Furthermore, the principle of non-discrimination signifies personal data that gives rise to unlawful or arbitrary discrimination may not be collected, such as information about racial or ethnic origin, colour, sex life, political opinions, religious, philosophical, and other beliefs, and membership in an association or trade union,[65] and the security principle means that appropriate measures must be taken to protect personal data from both natural dangers, such as accidental loss or destruction, and human dangers, such as unauthorized access, fraudulent misuse of data, or contamination by computer viruses.

Point 6 of the Guidelines states that exceptions to the first five principles may be made, in the case of national security, public order, public health or morality.

Three other points in the Guidelines are worth highlighting: First, although the Guidelines refer to personal data, they do not define personal data; second, the Guidelines indicate that the law of each country determines the authority that monitors compliance with the principles; the last point provides for a limitation on transborder data flows, which means that transborder data flows must be limited whether it is not possible to ensure the same principles that are provided for in the Guidelines.

At this juncture, it is also interesting to highlight the United Nations General Assembly Resolution 28/16 of 1 April 2015 adopted by the Human Rights Council,

---

[63] Ibid., point 3.

[64] Ibid., point 4.

[65] Ibid., point 5.

which concerns the right to privacy. Based on this resolution, the United Nations Human Rights Council introduced a Special Rapporteur on the right to privacy. The Special Rapporteur works to identify obstacles to promoting the right to privacy, develop and promote best practices, report alleged violations, and raise awareness of the right, bearing in mind the influence of new technologies. This shows that even the United Nations pays great attention to the issue of data protection and privacy protection.

4. APEC Privacy Framework

The Asia-Pacific Economic Cooperation (APEC) is an intergovernmental forum established in 1989. To date, it has 21 member economies,[66] promoting free trade throughout the Asia-Pacific region. Today, the APEC economies represent more than a third of the world's population and half of the world's GDP in trade.[67]

The ministers of the APEC economies in November 2004, during their meeting, adopted the Privacy Framework finalized in 2005, called the APEC Privacy Framework.[68] It was developed between 2003 and 2004 by APEC's Electronic Commerce Steering Group (ECSG) Privacy Subgroup and was updated in 2015.

The APEC Privacy Framework does not apply as law, so it is not binding on APEC member economies; it is only a suggestion, setting out the basic principles for minimum personal information standards that APEC member economies agree to use to establish or amend their national legislation. In the absence of national legislation or where the applicable law provides less protection for information

---

[66] Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; the Philippines; the Russian Federation; Singapore; Chinese Taipei; Thailand; the United States of America; Vietnam.

[67] G. Greenleaf, *Five years of the APEC Privacy Framework: Failure or promise?*, Computer Law & Security Review, no. 25, 2009.

[68] Asia–Pacific Economic Cooperation (APEC), Privacy Framework, 2005.

subjects,[69] the APEC Privacy Framework governs personal information and not personal data.[70]

The APEC Privacy Framework aims to develop appropriate personal information privacy and ensure the free flow of personal information in the Asia Pacific region, even though APEC member economies do not recognise the right to personal information protection as an individual and fundamental right.[71]

The APEC Privacy Framework is divided into four parts. Parts I and II address the preamble and scope, and Part III consists of a set of nine APEC Information Privacy Principles, namely preventing harm,[72] notice,[73] collection limitations,[74] uses of personal information,[75] choice,[76] the integrity of personal information,[77] securi-

[69] C. Sullivan, *EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfer and protection of personal data in the IoT era*, Computer Law & Security Review, no. 35, 2019.

[70] See, Part 2, Chapters 1, 2, and 3.

[71] See, APEC Privacy Framework, Part I, Preamble.

[72] The principle of preventing harm is one of the primary objectives of the Framework which states that personal information protection should be designed to prevent the misuse of such information.

[73] The principle of notice suggests that personal information controllers should provide clear and easily accessible statements about their personal information practices and policies.

[74] The principle of collection limitations notes that personal information collection should be limited to information that is relevant for the purposes of collection and should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.

[75] The principle of uses of personal information provides that personal information should only be used to fulfil the purposes of collection and for other compatible or related purposes.

[76] The principle of outlines that individuals should be provided with clear, prominent, easily understandable, accessible, and affordable methods to exercise their choice in relation to the collection, use, and disclosure of their personal information. However, it may not be necessary to provide these methods when collecting publicly available information.

[77] The principle of the integrity of personal information requires personal information to be kept accurate, complete, and up to date to the extent necessary for utilisation purposes.

ty safeguards,[78] access and correction,[79] and accountability.[80] Part IV concerns implementation including Part A "Guidance on Domestic Implementation" and Part B "International Implementation".

The APEC Leaders, under the APEC Privacy Framework, developed in 2007, created several Pathfinder projects for cross-border data transfers and endorsed the APEC Cross Border Privacy Rules System (CBPR System) in 2011 to build trust among consumers, businesses, and regulators in the flow of personal information across borders.[81] The CBPR System is a privacy certification that companies or governments can join to demonstrate compliance with internationally recognised privacy protections, particularly compliance with the nine APEC Information Privacy Principles.[82]

In addition, by the APEC Privacy Framework, Part IV, Part B, APEC member economies are called upon to consider developing cooperative arrangements and procedures to facilitate cross-border cooperation in the enforcement of privacy laws. In 2009, the APEC member economies developed the Cooperation Arrangement for Cross-Border Privacy Enforcement (CPEA).[83] This arrangement

---

[78] The principle of security safeguard provides that personal information controllers adopt appropriate safeguards against risks such as loss, unauthorised access, or unauthorised destruction, use, modification, or disclosure of information, as well as other misuses to protect the personal information in their possession.

[79] The principle of access and correction includes specific conditions for what would be considered reasonable in the provision of access, including conditions related to timing, fees, and the manner and form in which access would be provided.

[80] The principle of accountability provides that personal information controllers should be accountable for complying with measures that give effect to the APEC Information Privacy Principles.

[81] Asia–Pacific Economic Cooperation, APEC Cross-Border Privacy Rules Systems Policies, Rules and Guidelines, November 2019.

[82] Ibid.

[83] Asia–Pacific Economic Cooperation, APEC Cooperation Arrangement for Cross-Border Privacy Enforcement, 2010/SOM1/ECSG/DPS/013, 2010.

serves as an excellent example of a regional multilateral arrangement developed by the APEC member economies.[84]

[84] Organisation for Economic Co-operation and Development, Report on the implementation of the recommendation of the council on cross-border co-operation in the enforcement of laws protecting privacy [C(2007)67/FINAL], C(2011)51, 29 March 2011.

Chapter 2
The EU Sources of Personal Data Protection Law

The European Union (EU) has a comprehensive legal framework for the protection of personal data. Although international communities introduced the first standards for personal data and influenced the first phase of the lawmaking of EU legal instruments on personal data protection, the EU has always been a pioneer in digital and technological laws, as the rules introduced by the EU are binding and progressive. For example, the EU recognises the right to the protection of personal data as distinct from the right to privacy, which has a solid basis in the EU Treaties and has developed a new approach, called the content-purpose-result approach, which replaces the privacy approach used by international communities to decide whether there is a violation of the right to the protection of personal data.[85] Another example is the approved proposal for an EU regulation on artificial intelligence (AI Act), which will be the first law in the world to dictate to companies how they can use artificial intelligence. Additionally, the European Commission (EC) presented the Digital Single Market Strategy (DSM Strategy) on 6 May 2015. With this strategy, the EU aims to remain among the world leaders in the digital economy and support the growth of European companies globally.[86]

This part will explain the sources of personal data protection law in the EU. Specifically, it will describe, from a personal data protection perspective, the Charter of Fundamental Rights of the EU, the EU Treaties, the General Data Protection Regulation (GDPR) and its predecessor Directive 95/46/EC (DPD). It will also briefly discuss the significant jurisprudence of the Court of Justice of the Europe-

[85] See, Part 2, Chapter 4, Paragraphs 1-2.

[86] SWD (2015) 100-final, Commission staff working document "A Digital Single Market Strategy for Europe – Analysis and Evidence", Accompanying the document, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, of 6 May 2015.

an Union (CJEU) and the ongoing proposals regarding the AI Act and the ePrivacy Regulation.

1. Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union (EU CFR) not only respects private and family life, the so-called right to privacy but also recognises the right to the protection of personal data in Article 8. This enshrines the right to the protection of personal data as an individual fundamental right in the EU legal order. Under article 7, "*everyone has the right to respect for his or her private and family life, home and communications*". Article 8, Paragraph 1 states that "*everyone has the right to the protection of personal data concerning him or her*". According to Paragraph 2 of Article 8, "*such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law,*" and "*everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified*", the Paragraph 3 of Article 8 specifies that "*compliance with these rules shall be subject to control by an independent authority*".

Articles 7 and 8 of the EU CFR shall be read in conjunction with other provisions of the same Charter. Article 51, Paragraph 1, institutions and bodies of the Union and the EU Member States shall respect and guarantee the rights enshrined in the EU CFR. Furthermore, Article 52, Paragraph 1, states that "…*limitation on the exercise of the rights and freedoms recognised by this Charter*…". It continues affirming limitation can be possible only by respecting "*the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*". An example case could be the case of *Schecke* in

2010,[87] in which the Court of Justice of the European Union (CJEU) stated, "*The right to the protection of personal data is not, however, an absolute right, but must be considered in relation to its function in society*".[88]

The CJEU makes a clear distinction between the right to privacy and the right to the protection of personal data, and this distinction is also applied to its cases. One of the most significant cases in the EU legal order is the *Google Spain v AEPD and Mario Costeja González* case.[89] It states, "*Processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name*".[90]

2. European Union Treaties

Among the relevant rules in the EU treaties include Article 39 of the Treaty on the European Union (TEU) and Article 16 of the Treaty on the Functioning of the European Union (TFEU).

Article 16, Paragraph 1 of the TFEU expressly provides everyone has the right to personal data protection. Paragraph 2 establishes "*The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and*

---

[87] See, Judgment of the CJEU, of Grand Chamber, of 9 November 2010, Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen, Joined cases C-92/09 and C-93/09, ECLI:EU:C:2010:662.

[88] Ibid., Paragraph 48.

[89] See, Judgment of the CJEU, of Grand Chamber, of 13 May 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, case C-131/12, ECLI:EU:C:2014:317.

[90] Ibid., Paragraph 80.

by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities".

Article 39 of the TEU extends the right to personal data protection also to the specific sector of the Common Foreign and Security Policy (CFSP),[91] envisaged in this field the decision taken by the Council "*in accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities*".

3. *Directive 95/46/EC on the Protection of Individuals about the Processing of Personal Data and on the Free Movement of Such Data (Data Protection Directive)*

Directive 95/46/EC, also known as the Data Protection Directive (DPD), on the protection of individuals regarding the processing of personal data and the free movement of such data, was enacted in October 1995 and came into force on 13 December 1995.[92] It was replaced on 25 May 2018.

The DPD regulated data protection at the EU level for the first time and aimed at putting into practice in the EU the principles already contemplated in OECD Pri-

[91] The Common Foreign and Security Policy (CFSP) is the organised, agreed foreign policy of the European Union (EU) for mainly security and defence diplomacy and actions.

[92] Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J.E.C. L 281/31, of 23 November 1995.

vacy Guidelines and Convention 108,[93] so they could be considered a cornerstone for the European framework on personal data protection.[94] The DPD is also known as the "mother Directive",[95] since it restricts the collection and use of personal data and requires the EU Member States to establish an independent national body in charge of the protection of such data, which has led to the emergence of national data protection authorities. Like all EU directives, the DPD must be transposed before it can be incorporated into the legal system of the EU Member States.

The DPD aims to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy, with respect to the processing of personal data.[96]

Articles 6 and 7 of the DPD lay down a set of fundamental principles relating to data quality and the legitimacy of data processing. Under Article 6 the EU Member States shall provide that personal data must be: "*a) processed fairly and lawfully; b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical, or scientific use*". The personal data controller must en-

[93] See, Focarelli, *La privacy. Proteggere i dati personali oggi*, p. 117.

[94] C. De Terwangne, *Council of Europe convention 108+: A modernized international treaty for the protection of personal data*, Computer Law & Security Review, no. 40, 2021.

[95] See, Focarelli, *La privacy. Proteggere i dati personali oggi*, p.p. 117-118.

[96] See, Directive 95/46/EC, Article 1.

sure that it complied with these requirements. Pursuant to Article 7, the EU Member States shall provide that personal data may be processed only if: "*a) the data subject has unambiguously given his consent; or b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or c) processing is necessary for compliance with a legal obligation to which the controller is subject; or d) processing is necessary in order to protect the vital interests of the data subject; or e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1*".

Based on Article 29 of the DPD, a working party on the protection of personal data, the so-called Article 29 Working Party (WP29), was formed. It was composed of representatives of the various EU national authorities, the European Data Protection Supervisor (EDPS),[97] and a representative of the EU Commission. Its main tasks were to interpret the DPD, provide technical advice to EU Member States on data protection issues, promote the consistent application of the DPD in all EU Member States as well as in Norway, Liechtenstein and Iceland, issue an opinion on Community legislation affecting the right to the protection of personal data, and make recommendations to the public on issues relating to the protection of individuals concerning the processing of personal data and privacy at European

[97] The European Data Protection Supervisor (EDPS) is an independent supervisory authority established in accordance with Regulation (EU) No 2018/1725, based on Article 16 TFEU. Do not be confused with the European Data Protection Board (EDPB), which is an independent European body composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS).

level.[98] During its mandate, the WP29 issued numerous opinions and recommendations that have guided EU member states in the application of the DPD. Due to the large number of opinions and recommendations issued, they are analysed in this paper as necessary.

Since the GDPR entered into force in the EU legal order, the WP29 has been replaced by the European Data Protection Board (EDPB). In 2010 the Commission set out its approach to modernising the EU legal framework for data protection in its Communication "*A comprehensive approach on personal data protection in the European Union*".[99] It emphasised the role of supervisory authorities and the WP29 but noted that data protection authorities continue to apply and interpret EU rules differently. The EU Commission, therefore, called for the "*strengthening of the Working Party's role in coordinating DPAs' positions, ensuring a more uniform application at the national level and thus an equivalent level of data protection*". It conducted an analysis, including "*How to ensure a more consistent application of EU data protection rules across the internal market. This may include strengthening the role of national data protection supervisors, better coordinating their work via the Article 29 Working Party (which should become a more transparent body), and/or creating a mechanism for ensuring consistency in the internal market under the authority of the European Commission*".[100]

---

[98] See, Directive 95/46/EC, Article 30.

[99] COM(2010) 609 final, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union*, of 4 November 2010.

[100] Ibid., p.p. 17-18.

4. General Data Protection Regulation (GDPR)

On 27 April 2016, the European Union adopted the General Data Protection Regulation (GDPR).[101] It entered into force on 25 May 2018. The GDPR Proposal started on 25 January 2012,[102] so it took more than four years after the EU Commission proposed it. The EU Commission stated that "*The EU needs a more comprehensive and coherent policy on the fundamental right to personal data protection*", due to "*Rapid technological developments have brought new challenges for the protection of personal data*".[103] The EU Commission urged that it is necessary to ensure a consistent and high level of personal data protection,[104] and the level of personal data protection in the EU must be equivalent between EU Member States,[105] so a Regulation could achieve better this goal than a Directive since an EU Regulation is a binding legislative act, which does not need transposition. Indeed, some commentators affirm that the GDPR represents a step change in data protection law both in Europe and internationally.[106] One reason is that it is directly applied and must be applied across the EU Member States' legal systems. Another reason is that the GDPR restricts cross-border data transfers, directly regu-

---

[101] Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), O.J.E.U. L 119/1, of 4 May 2016.

[102] COM(2012) 11 final, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, of 25 January 2012.

[103] Ibid., p.p. 1-2.

[104] See, EU Commission Communication, COM(2010) 609 final, p.p. 4-5.

[105] E. S. Dove, *The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era*, The Journal of Law, Medicine & Ethics, no. 46, 2018.

[106] J.P. Albrecht, *How the GDPR Will Change the World*, European Data Protection Law Review 2, no. 3, 2016.

lating the conduct of many non-EU organisations, and influences data protection legislation around the world, thus, having a global impact.[107]

The reason the EU adopted a directive instead of a regulation in 1995 that there were disparities existed between EU Member States, and adopting a regulation could have undermined the EU common market.[108] Today, the social context is different due to rapid technological development, so it is necessary to have equivalent and homogeneous standards. Therefore, the GDPR is a milestone in the development of the EU data protection framework.[109]

The key principles of the GDPR are lawfulness, fairness, transparency, [110] purpose limitation,[111] minimisation,[112] data accuracy,[113] storage limitation,[114] integrity and confidentiality,[115] and accountability principles.[116]

---

[107] C. Kuner, D. Jerker, B. Svantesson, F. H. Cate, O. Lynskey, C. Millard and N. N. Loideain, *The GDPR as a chance to break down borders, International Data Privacy Law*, 2017, Vol. 7, No. 4, 2017.

[108] See, Directive 95/46/EC, Article 30, recitals 7 and 8.

[109] M. Goddard, *The EU General Data Protection Regulation (GDPR): European regulation that has a global impact*, International Journal of Market Research Vol. 59 Issue 6, 2017.

[110] See, GDPR, Article 5, Paragraph 1, lett. a: *processed lawfully, fairly and in a transparent manner in relation to the data subject*.

[111] See, GDPR, Article 5, Paragraph 1, lett. b: *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 Paragraph 1, not be incompatible with the initial purposes*.

[112] See, GDPR, Article 5, Paragraph 1, lett. c: *adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed*.

[113] See, GDPR, Article 5, Paragraph 1, lett. d: *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay*.

[114] See, GDPR, Article 5, Paragraph 1, lett. e: *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be pro-*

Comparing the DPD and the GDPR, there is an expansion in size; the GDPR is a huge text,[117] contains 99 articles of the 34 articles of the DPD. Many of its provisions replicate the DPD or reflect pre-existing jurisprudence and administrative practice.[118] Principles of personal data processing under the GDPR are like the DPD, but there are a few differences. For example, the transparency requirement explicitly for the processing of personal data, which is provided for in Article 5, Paragraph 1, letter A, compared to the DPD, was only implicit.[119] Additionally, the GDPR adds a time element to the accuracy principle. The GDPR requires that inaccurate personal data must be erased or rectified without delay. Finally, the GDPR introduced joint responsibility; under the DPD, only data controllers were held accountable for any improper processing of personal data, whereas, under the GDPR, both data controllers and data processors are jointly responsible.[120]
There are other differences compared to the DPD; the GDPR provides a more extensive definition of personal data, including more information.[121] The GDPR

---

cessed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 Paragraph1 subject to the implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

[115] See, GDPR, Article 5, Paragraph 1, lett. f: *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures*.

[116] See, GDPR, Article 5, Paragraph 2: *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1*.

[117] C. Kuner, L. A. Bygrave, C. Docksey, *Background and Evolution of the GDPR,* in The EU General Data Protection Regulation: A Commentary, Oxford University Press, 2020.

[118] Ibid., p. 2.

[119] W. G. Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, Business Lawyer, American Bar Association, 2017.

[120] See, GDPR, Article 5, Paragraph 2.

[121] See, Part 2, Chapter 2, Paragraphs 1-2.

gives data subjects rights over their data.[122] The GDPR has introduced stringent protocols for data breaches and penalties,[123] and the GDPR has a broader territorial reach, as outlined in Article 3, which grants it extraterritorial applicability.

Furthermore, Recital 4 of the GDPR outlines the social purpose of the regulation. Specifically, it states, "*The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity*." The phrase "*to serve mankind*" underscores the notion that the processing of personal data should be directed towards benefiting humanity. Simply put, the utilization of personal data should have a positive impact on society and contribute to the common good. In essence, Recital 4 establishes a philosophical and ethical foundation for the GDPR, accentuating the importance of responsible and ethical handling of personal data within the overarching framework of safeguarding fundamental rights and freedoms.[124]

---

[122] See, Part 4, Chapter 2.

[123] See, Part 5, Chapter 2, Paragraph 2.

[124] H. Hijmans and C. Raab, *Ethical Dimensions of the GDPR*, *in: Mark Cole and Franziska Boehm, Commentary on the General Data Protection Regulation*, Cheltenham, Edward Elgar, 2018, pages 1-8.

5. *Proposals: Regulation concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications (E-Privacy Regulation), and Regulation on Artificial Intelligence (AI ACT)*

The will of the EU is to remain a leader in the digital economy. The EU is considered a pioneer in digital legislation not only due to the existence of the former DPD and current GDPR, but it has several legal instruments that ensure the protection of fundamental rights and freedoms in the electronic environment. For example, in the EU legal order, there is an ePrivacy Directive,[125] which ensures the protection of fundamental rights and freedoms, in particular the respect for private life, the confidentiality of communications, and the protection of personal data in the electronic communications sector. The EU Commission announced the Digital Single Market Strategy for Europe (DSM Strategy),[126] which consists of revising the ePrivacy Directive, seeking to provide a high level of privacy protection for users of electronic communications services and a level playing field for all market players. Two years after the announcement of the DSM Strategy, in 2017, the EU Commission launched a proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications, known as the Proposal for an ePrivacy Regulation, which would repeal the ePrivacy Directive.[127]

---

[125] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J.E.C. L201/37, of 31 July 2002.

126 The Digital Single Market strategy was adopted on 6 May 2015 and is one of the European Commission's 10 political priorities. It is made up of three policy pillars: 1. Improving access to digital goods and services; 2. An environment where digital networks and services can prosper; 3. Digital as a driver for growth.

[127] COM(2017) 10 final, *Proposal for a Regulation of the European Parliament and of the Council, concerning the respect for private life and the protection of personal data in electronic communi-*

Another significant example is the ongoing proposal of the EU on Artificial Intelligence (AI). It will become the first legal instrument of Artificial Intelligence in the world.[128] According to the EU Commission's opinions, AI is no longer fiction; it is increasingly close to our daily lives, which means personal data is easily violated. Owing to AI being closely related to personal data, or to data in general, without data, Artificial Intelligence is not able to work. Therefore, on 21 April 2021, the EU Commission presented the Artificial Intelligence Act (AI Act).[129] This proposal was approved by the European Parliament on 14 June 2023 with 499 votes in favor, 28 against, and 93 abstentions. It is expected to enter into force in 2024.

The proposal defines the common mandatory requirements applicable to the design and development of certain AI systems before they are placed on the market, and the situation after the AI systems have been placed on the market, by harmonising the way ex-post controls are carried out. Furthermore, this proposal contains some specific rules on the protection of natural persons regarding the processing of personal data, in particular restrictions on the use of AI systems for "real-time" remote biometric identification in spaces accessible to the public for contrast purposes.[130] According to Article 3, paragraph 37 of the Draft AI Act, "real-time" remote biometric identification means "*a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay*". This comprises not only instant identification but also limited short delays to avoid circumvention.

---

cations and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), of 10 January 2017.

[128] European Parliament, AI Act: a step closer to the first rules on Artificial Intelligence, of 11 May 2023.

[129] COM(2021) 206 final, *Proposal for a Regulation of the European Parliament and of the Council, Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence ACT)*, of 21 April 2021.

[130] See, Proposal Artificial Intelligence ACT, page 6.

Furthermore, it is necessary to clarify that the two proposals, the ePrivacy and AI Acts, are based on Article 16 of the TFEU, like the GDPR. Article 16 of the TFEU regulates the right to the protection of personal data. This shows how closely and compatibly Artificial Intelligence and Privacy are related to the protection of personal data.

Chapter 3
The Chinese Sources of Personal Information Protection Law

China is a country with a large population and one of the most important leaders in the digital economy in the world, but it is not the vanguard of digital law. Indeed, its history of personal information protection legislation is very young.

The first Chinese Personal Information Protection Law (PIPL) entered into force on 1st November 2021.[131] In the PIPL, the Chinese legislator regulates personal information and not personal data. Obviously, "information" and "data" are two different words, even though in many contexts they are used as synonyms.[132]

Before the PIPL went into effect, there was a lot of uncertainty about the status of personal information in the Chinese legal system,[133] owing to there being no real right to personal information protection. Personal information has been mentioned in several Chinese laws, which state that personal information needs to be protected, but the right to personal information protection is still only a theoretical right.

The first time the right to personal information protection was written into a Chinese law was in 2013 when the Chinese legislators published the Chinese Law of Protection of Consumer Rights and Interests (PCRI).[134] Particularly under Articles 14 and 29. Article 14 of the PCRI states "*When consumers purchase and use goods and receive services, they have the right to respect their personal dignity*

---

[131] Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ (中华人民共和国个人信息保护法, the Chinese Personal Information Protection Law), of the 30th Meeting of the Standing Committee of the 13th National People's Congress of the Republic of China, of 20 August 2021.

[132] See, Part 2, Chapters 2-3.

[133] W. Shen, *On the Construction and Systematization of the Personal Information Right (论个人信息权的构建及其体系化)*, Journal of Comparative Law (比较法研究), No.5, 2021.

[134] Zhōnghuá rénmín gònghéguó xiāofèi zhě quányì bǎohù fǎ (中华人民共和国消费者权益保护法, Chinese Law of Protection of Consumer Rights and Interests), of the 5th Meeting of the Standing Committee of the 12th National People's Congress of the People's Republic of China, of 25 October 2013.

and ethnic customs, and the right to protect their personal information in accordance with the law".[135] Article 29, Paragraph 1 of the PCRI describes the principles to be respected in the processing of personal information, especially recalls "*When collecting and using consumers' personal information, business operators shall follow the principles of legality, legitimacy, and necessity, expressly state the purpose, method and scope of the collection and use of information, and obtain the consent of consumers. Business operators shall disclose their collection and use rules when collecting and using consumers' personal information and shall not collect and use information in violation of the provisions of laws and regulations and the agreement of both parties*",[136] Paragraph 2 continues to regulate "*Business operators and their staff must keep the collected personal information of consumers strictly confidential, and must not disclose, sell, or illegally provide it to others. Business operators shall take technical measures and other necessary measures to ensure information security and prevent leakage and loss of consumers' personal information. When information leakage or loss occurs or may occur, remedial measures shall be taken immediately*",[137] Paragraph 3 concludes "*Business operators shall not send commercial information to consumers without their consent or request, or if consumers had expressly refused*".[138]

---

[135] Translated by the author, the original text is "消费者在购买, 使用商品和接受服务时, 享有人格尊严, 民族风俗习惯得到尊重的权利, 享有个人信息依法得到保护的权利".

[136] Translated by the author, the original text is "经营者收集,使用消费者个人信息, 应当遵循合法, 正当, 必要的原则, 明示收集, 使用信息的目的, 方式和范围, 并经消费者同意. 经营者收集, 使用消费者个人信息, 应当公开其收集, 使用规则, 不得违反法律, 法规的规定和双方的约定收集, 使用信息".

[137] Translated by the author, the original text is "经营者及其工作人员对收集的消费者个人信息必须严格保密, 不得泄露, 出售或者非法向他人提供. 经营者应当采取技术措施和其他必要措施, 确保信息安全, 防止消费者个人信息泄露, 丢失. 在发生或者可能发生信息泄露, 丢失的情况时, 应当立即采取补救措施".

[138] Translated by the author, the original text is "经营者未经消费者同意或者请求, 或者消费者明确表示拒绝的, 不得向其发送商业性信息".

Subsequently, the Chinese Cybersecurity Law (CSL) also regulated the protection of personal information in 2016.[139]

Before the enactment of the PIPL, the CSL had been the main law to protect personal information, due to its relative completeness of personal information protection rules. Under the CSL, there are nine Articles regarding personal information, which are Article 22, Paragraph 3 about the consent of the information subject,[140] Article 37 on personal information extraterritorial transfers,[141] Article 41 regarding the principles of personal information processing,[142] Article 42 listing the ob-

---

[139] Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ (中华人民共和国网络安全法, Chinese Cybersecurity Law), of the 24th Meeting of the Standing Committee of the 12th National People's Congress of the People's Republic of China, of 7 November 2016.

[140] Translated by the author, translated version "*Where network products and services have the function of collecting user information, their providers shall expressly indicate to users and obtain consent; if personal information of users is involved, they shall also abide by the provisions of this Law and relevant laws and administrative regulations on the protection of personal information*". The original text is "网络产品, 服务具有收集用户信息功能的, 其提供者应当向用户明示并取得同意; 涉及用户个人信息的, 还应当遵守本法和有关法律, 行政法规关于个人信息保护的规定".

[141] Translated by the author, translated version "*The personal information and important data collected and generated by the operators of key information infrastructure during their operations within the territory of the People's Republic of China shall be stored within the territory of the People's Republic of China. If it is really necessary to provide overseas due to business needs, a security assessment shall be conducted in accordance with the measures formulated by the national network information department in conjunction with the relevant departments of the State Council; where laws and administrative regulations provide otherwise, follow their provisions*". The original text is "关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储. 因业务需要, 确需向境外提供的, 应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估; 法律, 行政法规另有规定的, 依照其规定".

[142] Translated by the author, translated version "*When collecting and using personal information, network operators shall follow the principles of legality, justification, and necessity, disclose the collection and use rules, expressly state the purpose, method and scope of the collection and use of information, and obtain the consent of the person being collected. Network operators shall not col-*

ligations of network operators (information controllers),[143] Articles 43 and 44 governing the rights of information subjects,[144] Article 45 stating the responsibil-

---

lect personal information irrelevant to the services they provide, shall not collect and use personal information in violation of the provisions of laws and administrative regulations and the agreement between the two parties, and shall process their storage in accordance with the provisions of laws and administrative regulations and the agreement with users. personal information". The original text is "网络运营者收集, 使用个人信息, 应当遵循合法, 正当, 必要的原则, 公开收集, 使用规则, 明示收集, 使用信息的目的, 方式和范围, 并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息, 不得违反法律, 行政法规的规定和双方的约定收集, 使用个人信息, 并应当依照法律, 行政法规的规定和与用户的约定, 处理其保存的个人信息".

[143] Translated by the author, translated version "*Network operators must not disclose, tamper with, or damage the personal information they collect; they must not provide personal information to others without the consent of the person being collected. However, there is an exception for processing that cannot identify a specific individual and cannot be restored. Network operators shall take technical measures and other necessary measures to ensure the security of the personal information they collect and prevent information leakage, damage, or loss. When personal information leakage, damage, or loss occurs or may occur, remedial measures shall be taken immediately, and users shall be notified in a timely manner and reported to relevant competent authorities in accordance with regulations*". The original text is "网络运营者不得泄露, 篡改, 毁损其收集的个人信息; 未经被收集者同意, 不得向他人提供个人信息. 但是, 经过处理无法识别特定个人且不能复原的除外。网络运营者应当采取技术措施和其他必要措施, 确保其收集的个人信息安全, 防止信息泄露, 毁损, 丢失. 在发生或者可能发生个人信息泄露, 毁损, 丢失的情况时, 应当立即采取补救措施, 按照规定及时告知用户并向有关主管部门报告".

[144] Translated by the author, Article 43 translated version "*Individuals who discover that network operators have collected and used their personal information in violation of laws, administrative regulations, or the agreement between the two parties shall have the right to request that network operators delete their personal information; The right to request network operators to make corrections. Network operators should take measures to delete or correct*". The original text is "个人发现网络运营者违反法律, 行政法规的规定或者双方的约定收集, 使用其个人信息的, 有权要求网络运营者删除其个人信息; 发现网络运营者收集, 存储的其个人信息有错误的, 有权要求网络运营者予以更正. 网络运营者应当采取措施予以删除或者更正". Article 44 translated version "*No individual or organization shall steal or obtain personal information in other illegal ways, and shall not illegally sell or illegally provide personal information to others*". The original

ity of the supervisory authority of personal information,[145] Article 64 regulating the sanction imposed in the case of violation,[146] and Article 76 attempting to give

---

text is "任何个人和组织不得窃取或者以其他非法方式获取个人信息, 不得非法出售或者非法向他人提供个人信息".

[145] Translated by the author, translated version "*Departments and their staff that are legally responsible for network security supervision and management must keep personal information, privacy, and business secrets learned during the performance of their duties strictly confidential, and must not disclose, sell, or illegally provide them to others*". The original text is "依法负有网络安全监督管理职责的部门及其工作人员, 必须对在履行职责中知悉的个人信息, 隐私和商业秘密严格保密, 不得泄露, 出售或者非法向他人提供".

[146] Translated by the author, translated version "*Where network operators or providers of network products or services violate the provisions of Article 22, Paragraph 3, Articles 41 to 43 of this Law, and infringe upon the right to legal protection of personal information, the relevant competent department shall To order corrections, a warning may be given alone or in combination according to the circumstances, illegal gains may be confiscated, and a fine of not less than one time but not more than ten times the illegal gains shall be imposed; if there are no illegal gains, a fine of not more than one million yuan shall be imposed. The responsible person shall be fined not less than 10,000 yuan but not more than 100,000 yuan; if the circumstances are serious, they may also be ordered to suspend relevant business, suspend business for rectification, close the website, revoke relevant business licenses or revoke business licenses. Where, in violation of the provisions of Article 44 of this Law, stealing or obtaining in other illegal ways, illegally selling or illegally providing personal information to others does not constitute a crime, the public security organs shall confiscate the illegal gains and impose a fine of more than ten times the amount of the illegal gains. For the following fines, if there is no illegal gain, a fine of not more than one million yuan shall be imposed*". The original text is "网络运营者, 网络产品或者服务的提供者违反本法第二十二条第三款, 第四十一条至第四十三条规定, 侵害个人信息依法得到保护的权利的, 由有关主管部门责令改正, 可以根据情节单处或者并处警告, 没收违法所得, 处违法所得一倍以上十倍以下罚款, 没有违法所得的, 处一百万元以下罚款, 对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款; 情节严重的, 并可以责令暂停相关业务, 停业整顿, 关闭网站, 吊销相关业务许可证或者吊销营业执照. 违反本法第四十四条规定, 窃取或者以其他非法方式获取, 非法出售或者非法向他人提供个人信息, 尚不构成犯罪的, 由公安机关没收违法所得, 并处违法所得一倍以上十倍以下罚款, 没有违法所得的, 处一百万元以下罚款".

a restrictive definition of personal information.[147] The CSL is still in effect, but these rules are now also contained in the PIPL in a more detailed and less restrictive way.

The Chinese legislators began to recognise the importance of regulating personal information, so in 2017 when the General Provisions of the Chinese Civil Code were published,[148] provided the right to personal information under Article 111, which states "*Personal information of natural persons is protected by law. Any organization or individual that intends to obtain others' personal information shall act in accordance with the law and ensure its security. No one shall illegally collect, use, process, or transmit the personal information of others, and shall not illegally buy, sell, provide to others, or publicize such information*".[149] Article 110, Paragraph 1 of the General Provisions of the Chinese Civil Code lists the right to privacy, which affirms "*Natural persons enjoy the right to life, body, health, name, portrait, reputation, honour, privacy, marriage autonomy and other rights*".[150] The CSL and the General Provisions of the Chinese Civil Code have

---

[147] Translated by the author, translated version "*Personal information refers to various information recorded electronically or in other ways that can identify a natural person's personal identity alone or in combination with other information, including but not limited to the natural person's name, date of birth, ID number, personal biometric information, address, phone number etc*". The original text is "个人信息, 是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息, 包括但不限于自然人的姓名, 出生日期, 身份证件号码, 个人生物识别信息, 住址, 电话号码等".

[148] Zhōnghuá rénmín gònghéguó mínfǎ zǒngzé (中华人民共和国民法总则, General Provisions of the Civil Law of the People's Republic of China), of the 5th Session of the 12th National People's Congress of the People's Republic of China, of 15 March 2017.

[149] Translated by the author, the original text is "自然人的个人信息受法律保护. 任何组织和个人需要获取他人个人信息的, 应当依法取得并确保信息安全, 不得非法收集, 使用, 加工, 传输他人个人信息, 不得非法买卖, 提供或者公开他人个人信息".

[150] Translated by the author, the original text is "自然人享有生命权, 身体权, 健康权, 姓名权, 肖像权, 名誉权, 荣誉权, 隐私权, 婚姻自主权等权利".

been extremely important in the progress of Chinese personal information protection development, contributing to radical changes. Before 2017, in China, the right to personal information protection was considered a part of the right to privacy,[151] as in the current international legal order. This case has been called the one-dimensional model in China.[152] After 2017, when the CSL and the General Provisions of the Chinese Civil Code came into force, the situation began to change; the right to privacy and the right to personal information protection were distinguished. The General Provisions of the Chinese Civil Code divide the right to privacy and the right to personal information protection into two different articles, which is called the dual-dimensional model. Therefore, the one-dimensional model has been replaced by the dual-dimensional model.[153] The dual-dimension model, like the EU legal order, recognises the right to privacy and the right to the protection of personal information as two individual rights.

Chinese legislators understand the need to protect personal information and have implemented rules to protect it everywhere. In 2018, China released the Chinese E-Commerce Law,[154] this law includes six articles that regulate how electronic commerce operators should protect the personal information of their customers. Articles 5 and 32 of the Chinese E-Commerce Law emphasize that e-commerce operators must ensure the right to personal information protection for their cus-

---

[151] L. Wang, *Legal Protection of Personal Information: Centered on the Line between Personal Information and Privacy (论个人信息权的法律保护-以个人信息权与隐私权的界为中心)*, Modern Law Science, Vol. 35, No. 4, 2013.

[152] Y. Li, *The Research on the "Dual System" Protection and Claim Basis of the Personal Privacy and Information in The General Principles of Civil Law (论《民法总则》中个人隐私与信息的"二元制"保护及请求权基础)*, Journal of Zhejiang Gongshang University, No. 3 General no. 144, 2017.

[153] Ibid., page 14.

[154] Zhōnghuá rénmín gònghéguó diànzǐ shāngwù fǎ （中华人民共和国电子商务法， Chinese E-Commerce Law）of the 5th Meeting of the Standing Committee of the 13th National People's Congress of the People's Republic of China, of 31 August 2018, Article 5.

tomers. Article 23 states electronic commerce operators must collect and use personal information following the personal information standards and administrative law. Article 25 regulates relevant that, "*Where relevant competent authorities require e-commerce operators to provide relevant e-commerce data and information under laws and administrative regulations, the e-commerce operators shall provide them. Relevant competent departments should take necessary measures to protect the security of data information provided by e-commerce operators, and keep the personal information, privacy, and business secrets in it strictly confidential, and must not disclose, sell or illegally provide them to others*".[155] Article 79 regulates the sanctions in case of misuse of personal information, which states that the sanctions contained in the CSL apply. Furthermore, Article 87 makes clear that the e-commerce supervisory authority has the responsibility to protect personal information.

At this point, it is necessary to clarify that, since 2021, the General Provisions of the Chinese Civil Code are no longer in force; they have been replaced by the Chinese Civil Code.

In addition, the dual-dimensional model now represents the primary model on this matter. It has been incorporated into the Personal Information Protection Law and the Chinese Civil Code, which are the two main laws regulating and protecting personal information. The dual-dimensional model has also been confirmed by the Chinese court, which states that the right to privacy and the right to personal information protection are equal.[156] With the *Huang X v. Tencent Technology*

---

[155] Translated by the author, the original text is "有关主管部门依照法律, 行政法规的规定要求电子商务经营者提供有关电子商务数据信息的, 电子商务经营者应当提供. 有关主管部门应当采取必要措施保护电子商务经营者提供的数据信息的安全, 并对其中的个人信息, 隐私和商业秘密严格保密, 不得泄露, 出售或者非法向他人提供".

[156] See, Judgment of case *Luō X sù XX bǎoxiǎn gōngsī yǐnsī quán jiūfēn àn (罗某诉某某保险公司隐私权纠纷案, Luo X v. XX Insurance Company a dispute over infringement on the right to pri-*

(Shenzhen) Co., Ltd,[157] and *Ling XX v. Beijing Weibo Shijie Technology Co., Ltd* cases,[158] the Chinese court affirms that the right to privacy and the right to personal information protection are two individual civil rights, but complementary to each other.

1. Chinese Civil Code

On 28 May 2020, the National People's Congress of China adopted the first Civil Code (CC), which came into effect on 1 January 2021.[159] The CC stipulates the right to privacy and the right to protection of personal information in Chapter VI, which is about personality rights, meaning that Chinese legislators recognise the right to privacy and the right to protection of personal information as two rights of personality. In addition, the standard of the protection of personal information is also found under Article 111, in Chapter V, which regulates civil law rights. It is

---

vacy), 2014 Chēn běi mín èr chū zì dì 947 hào (2014 郴北民二初字第 947 号, 2014 Chenbei Min Er Chu no. 947), of 13 April 2015.

[157] See, Judgment of case *Huáng mǒu sù téngxùn kējì (shēnzhèn) yǒuxiàn gōngsī, téngxùn kējì (běijīng) yǒuxiàn gōngsī děng yǐnsī quán, gèrén xìnxī bǎohù jiūfēn àn (黄某诉腾讯科技(深圳)有限公司、腾讯科技(北京)有限公司等隐私权、个人信息保护纠纷案, Huang X v. Tencent Technology (Shenzhen) Co., Ltd)*, 2019 Jīng 0491 mín chū 16142 hào (2019 京 0491 民初 16142 号, 2019 Jing 0491 Min Chu no.16142), of 30 July 2020.

[158] See, Judgment of case *Líng mǒu mǒu sù běijīng wēi bō shìjiè kējì yǒuxiàn gōngsī yǐnsī quán, gèrén xìnxī quányì wǎngluò qīnquán zérèn jiūfēn àn (凌某某诉北京微播视界科技有限公司隐私权、个人信息权益网络侵权责任纠纷案，Ling XX v. Beijing Weibo Shijie Technology Co., Ltd)*, 2019 Jīng 0491 mín chū 6694 hào (2019 京 0491 民初 6694 号，2019 Jing 0491 Min Chu no. 6694), of 30 July 2020.

[159] Zhōnghuá rénmín gònghéguó mínfǎ diǎn (中华人民共和国民法典, the Civil Code of People's Republic of China).

stated that "*A natural person's personal information is protected by law*".[160] The same statement is also repeated in Article 1034 of the CC. This repetition means that the information subject in the event of damage resulting from a personal information breach, has the right to seek compensation through a civil action.
The CC is composed of 1260 Articles, and the rules on the right to personal information are taken from the CSL and the General Provisions of the Chinese Civil Code.

2. Chinese Personal Information Protection Law (PIPL)

On 20 August 2021, the first Chinese Personal Information Protection Law (PIPL) was issued and entered into force on 1 November 2021, laying out a comprehensive set of rules regarding the collection, use, processing, sharing, and extraterritorial transfer of personal information in China.[161] The PIPL represents the Chinese GDPR, and for China, it is also a bridge for international digital cooperation.[162]
The PIPL has an interaction with the CSL, but compared with the CSL, the PIPL has more precise and broader rules, which are able to better regulate the digital context. For example, the definition of personal information provided under the CSL is very limited and is no longer compatible with the current digital context.
There are only 74 Articles in the PIPL; it is a law formulated by drawing on international experiences and considering the Chinese context, so it is not a law copied from existing models. For example, sensitive personal data, according to the GDPR, includes personal information that discloses racial or ethnic origin, but in

[160] Translated by the National People's Congress (NPC), the original text is "自然人的个人信息受法律保护".

[161] Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ (中华人民共和国个人信息保护法, the Chinese Personal Information Protection Law), of the 30th Meeting of the Standing Committee of the 13th National People's Congress of the Republic of China, of 20 August 2021.

[162] D. Albrecht, *Chinese first Personal Information Protection Law in contrast to the European GDRP*, Computer Law Review International: A Journal of Information Law and Technology, 2022.

China, we classify such information as public information, resulting in a lack of protection.[163]

Although PIPL remains unaffected by other existing models, it bears a remarkable resemblance to APEC in its preference for terminology usage. For example, both instruments regulate personal information rather than personal data.

The PIPL, compared with other legal instruments on personal information, expands the scope of protection of personal information, stipulates the rights of individuals in the processing of personal information, strengthens protection obligations for personal information processors,[164] establishes protection rules for sensitive personal information, regulates the personal information processing behaviour of state agencies, and improves legal remedies for personal information. The following Parts will elaborate further on these points in greater detail.

Another intriguing point is to analyse the relationship between the PIPL and the CC. There are conflicting views among Chinese legal scholars regarding these two Chinese legal instruments governing the protection of personal information. According to a legal scholar, the PIPL is not a special law; rather, it is legislation with similar value to the Chinese Civil Code, but with certain distinct functions. For instance, the Chinese Civil Code is only used for civil compensation.[165] On the other hand, a legal scholar claims that the PIPL is a special law and the CC is a basic general law, that has a reciprocal function between them.[166] This opinion is considered more plausible since the Chinese Civil Code has a very broad regulation on the protection of personal information, such for example also regulating

---

[163] L. Wang, X. Ding, *On the Highlights, Characteristics and Application of Personal Information Protection Law (论《个人信息保护法》的亮点、特色与适用)*, The Jurist, no. 6, 2021.

[164] In the Chinese system, the term "information handler" corresponds to the role of a "data controller" in the international and EU systems.

[165] H. Zhou, *个人信息保护的法律定位 (Gèrén xìnxī bǎohù de fǎlǜ dìngwèi)*, Studies in Law and Business, Vol. 37, no. 3, 2020.

[166] L. Wang, 论《个人信息保护法》与《民法典》的适用关系 (Lùn "gèrén xìnxī bǎohù fǎ" yǔ "mínfǎ diǎn" de shìyòng guānxì), Huxiang Law Review, no. 1, 2021.

the principles to be respected for the processing of personal information, therefore it does not only contain compensation rights.

Conclusion of Part 1

The main goal of this Part was to determine the source of personal data protection laws in the legal frameworks of the EU and international legal orders, as well as the source of personal information protection regulations within the Chinese legal system. In addition, to compare and analyse them, to know their relation, and if some models had influenced others.

In the International legal order, there are four instruments from four different international organisations. Only one of them is a binding instrument, Convention 108. Even though the others are not binding, they have influenced many national legislations on personal data protection, particularly the OECD Privacy Guidelines, Convention 108, and the APEC Privacy Framework.

Convention 108 has taken over and developed the OECD principles, with the only difference being that the Council of Europe has them incorporated into a legally binding treaty.[167] The OECD Privacy Guidelines influenced Convention 108.[168] In addition, together, the OECD Privacy Framework and Convention 108, have influenced the EU legal order, particularly the DPD.[169] Furthermore, the APEC Privacy Framework has influenced the Chinese PIPL.

International legal standards on personal data are considered obsolete, and they are not coherent with the principle of maximising benefits and minimising costs, as technological development is faster than the legislative process.[170]

All four international instruments have been reviewed, as the revision work serves to adapt to the current context.

---

[167] See, Focarelli, *La privacy. Proteggere i dati personali oggi*, page 110.

[168] G. Greenleaf, *The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108*, International Data Privacy Law, Volume 2, Issue 2, 2012.

[169] L. A. Bygrave, Privacy and Data Protection in an International Perspective, Scandinavian Studies in Law, 2010, page 187.

[170] See, Focarelli, *La privacy. Proteggere i dati personali oggi*, page 106.

The EU has the most comprehensive and highest level of personal data protection in the world.[171] In 1995, the EU adopted the first Data Protection Directive, which was replaced by the GDPR in 2018, representing the moment of maximum harmonization. The GDPR is the third generation of the personal data protection legal instrument, and it is the most important one in the world due to its Regulation characteristic, which is directly applied to all EU Member States' national systems. The GDPR also seems to ensure extraterritorial jurisdiction since the deterritorialization of the Internet and international communications technology, which has given rise to acute jurisdictional questions regarding who may regulate online activities.[172]

The EU is a pioneer in the matter of digital law, dividing the right to personal data protection from the right to privacy. This new "model" has influenced the Chinese system, which also recognises the right to personal information protection and the right to privacy as two distinct rights. But, in the EU both rights are considered fundamental rights, as constitutional rights. Instead, in China, they are just considered two civil rights.

The Chinese legal instruments are very young compared with the international and EU legal instruments. Some legal scholars call the PIPL the Chinese version of the GDPR.

The PIPL bears a striking resemblance to the GDPR, yet it introduces some noteworthy distinctions. While both the GDPR and the PIPL have extraterritorial applicability, the GDPR places greater emphasis on the location of the business establishment, whereas the PIPL places more significance on the location of the personal information processing activities.

---

[171] K. Ishii, *Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects*, AI & Soc, 2019, page 515.

[172] C. Ryngaert and M. Taylor, *The GDPR as Global Data Protection Regulation?,* Cambridge University Press, 2020.

The PIPL has been influenced by the GDPR, for instance, adding the word “identifiable” to the definition of personal information. However, the PIPL has been influenced by all international legal instruments on personal data protection, as stated by the Chinese government, that the PIPL draws on the experiences of others while retaining distinctive Chinese characteristics.

PART 2
THE CONCEPT OF PERSONAL DATA AND PERSONAL INFORMATION

Personal data is the core of personal data protection legislation and has a precise meaning in legal instruments.[173] In different legal systems, it may have different concepts.

Knowing the exact concept of personal data is necessary for the correct enforcement of legal standards both for prediction and violation. For example, new technologies such as artificial intelligence, since AI technology works with data, require that personal data have much more restrictive standards than data in general. In case of violation, the consequences are even more serious.

The term "data" commonly refers to "digital information",[174] but in the legal context, legislator has adopted a broad interpretation, in the sense that data is not just information in an electronic format.

This means that the concept of personal data cannot be limited only to the definition given by law. Indeed, for this reason, it is easy to have a definition, but difficult to outline a concept for personal data.[175]

This Part has used the word "concept" and not "definition", as the definition is the one given by the legislators and the concept is something broader.

The definition of personal data was first adopted in 1980 under an international legal instrument. Since the EU did not adopt the DPD, the definition of personal data under international instruments had dominated the EU legal order.

---

[173] N. Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, Law, Innovation and Technology, Vol 10, No. 1, 40-81, 2018.

[174] T. Streinz, *The Evolution of European Data Law*, in *The Evolution of EU Law*, edited by Paul Craig and Gráinne de Búrca, Oxford University Press, 2021, pages 902-936.

[175] G. Finocchiaro, *Intelligenza Artificiale e protezione dei dati personali*, Giurisprudenza Italiana, July 2019.

In the Chinese legal system, there is no definition of personal data, yet Chinese legislators have chosen to regulate personal information. The words “data” and “information” are not synonymous. In general, “information” is the fruit of data processing[176], and “data” is the quantities, characters, or symbols on which a computer operates.

This Part seeks to provide an expanded view of the concept of personal data under international and EU legal instruments and of the concept of personal information under the Chinese legal system, helping to understand the correct meaning of the definitions given by legislators. The “expansion view” means the Part does not analyze only the definition of personal data and personal information, but also related concepts, such as the concept of sensitive data and sensitive information, the case of pseudonymisation and anonymisation. In addition, the research analyses will take into consideration the historical context, and consider relevant case law, where possible.

This Part is divided into five Chapters. The first explains the concept of personal data under international legal instruments; the second states the concept of personal data under the EU legal instruments, particularly under the GDPR; the third Chapter delimits the concept of personal information under the Chinese legal instruments; the fourth Chapter analyses approaches or model used to interpret the concept of personal data (information); the following Chapters interprets the concept of sensitive data and sensitive information under international, EU, and Chinese legal instruments; the last Chapter illustrates the situation of anonymisation and pseudonymisation under international, EU, and Chinese legal instruments. The Part will end with a comparative view of the different contexts mentioned, determining whether the terms "personal data" and "personal information" are synonymous or not, and if not, their differences.

[176] Ibid.

Chapter 1
The Concept of Personal Data under International Legal Instruments

1. The Concept of Personal Data under OECD Privacy Guidelines

In 1980, the international community elaborated a definition of personal data under the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (or OECD Privacy Guidelines).[177] The definition of personal data contained in the OECD Privacy Guidelines represents the first definition at the international level, but not at the national level.[178]

---

[177] Organisation for Economic Cooperation and Development (also known as OECD*), Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, on 23 September 1980.

[178] Sweden enacted the Data Act in 1973, which entered into force on 1 July 1974, which is the world's first national data protection law. This Data Act contained the definition of personal information, which means information concerning an individual; Germany enacted the German Bundesdatenschutzgesetz (BDSG) in 1977, a federal data protection act entered into force on 1 January 1978. The BDSG defines personal data as details on the personal or material circumstances of an identified or identifiable physical person; France enacted its first data protection act in 1978, Act No. 78-17 of 6 January 1978 on data processing, data files, and freedoms, which defines personal data shall mean information which in any way whatever, directly or otherwise, enables the natural persons to whom it applies to be identified, whether the processing is carried out by a natural person or by a legal person; Norway adopted first generation legislation in form of the Act relating to Personal Data Registers on 9 June 1978, which states personal information shall mean information and assessments which are, directly or indirectly, traceable to identifiable individuals, associations or foundations; Austria has passed the first data protection law in 1979, enacted in 1978, Austrian Data Protection Act defines only data, which is information stored on a data medium concerning an identified or with great probability identifiable

The OECD Privacy Guidelines defined personal data as "*any information that relates to an identified or identifiable individual*".[179]

This is a broad definition, and it is the same one adopted in the revised version of the 2013 OECD Privacy Guidelines,[180] so in this Chapter, the OECD Privacy Guidelines refers to both the 1980 and revised 2013 OECD Privacy Guidelines, the distinction should be made only when necessary.

The revision working group of OECD Privacy Guidelines suggested taking into consideration the situation of deidentification, [181] particularly not including de-identified data as personal data and defining the meaning of the word "identifiable".[182] Deidentification means removing or obscuring identifying characteristics of personal data to avoid the identification of an individual.

The suggestion of the revision working group of the OECD Privacy Guidelines not to include de-identification data as personal data had not been taken into consideration, as the OECD states that de-identification and anonymisation techniques are unable to eliminate the risk of privacy; indeed, the techniques could even increase the risk of privacy.[183] For example, providing a right of access and rectification concerning de-identified data or data that is not readily identifiable unintentionally increases privacy risks.

---

[179] Organisation for Economic Cooperation and Development (also known as OECD*), Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, on 23 September 1980, Annex to Recommendation, Part One General, Article 1, point b.

[180] Organisation for Economic Cooperation and Development (OECD), *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)*, C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79.

[181] F. H. Cate; P. Cullen; and V. Mayer-Schonberger, *Data Protection Principles for the 21st Century,* books by Maurer Faculty, 2013.

[182] Organisation for Economic Cooperation and Development (OECD), *Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines"*, OECD Digital Economy Papers, No. 229, OECD Publishing, Paris, 11 October 2013.

[183] Ibid., pages 10-11.

Instead, concerning the words "*identified*" and "*identifiable*", the OECD emphasised that it is difficult to make sense of information relating to identified or identifiable individuals, so these situations must be left to the regulation of each member country.[184]

In short, the definition of personal data under the revised 2013 OECD Privacy Guidelines and under the 1980 OECD Privacy Guidelines are the same.

Furthermore, the OECD Privacy Guidelines explain that only the data of a natural person can be considered personal data. This means that they do not apply to legal persons; therefore, all data that can be converted into information, by direct relating or indirect linkages, to a natural person are considered personal data.[185]

Finally, underlining that the OECD Privacy Guidelines are recommendations and not binding legal instruments.

2. The Concept of Personal Data under Convention 108

The Convention for the Protection of Individuals regarding Automatic Processing of Personal Data (Convention 108) is the first and currently the only legally binding international instrument in personal data protection. Due to its binding efforts, legal scholar states the first definition of personal data was given by Convention 108.[186]

According to Convention 108, personal data is "*any information relating to an identified or identifiable natural person*".[187] This definition has been confirmed in the modernised version of Convention 108.

Convention 108 is not applied to deceased persons or legal persons, but the Explanatory Report of the Modernised Convention 108 provides an exception for le-

---

[184] See, 2013 OECD Privacy Guidelines, page 52.

[185] Ibid.

[186] C. Kuner, *An international legal framework for data protection: Issues and prospects*, Computer Law & Security Review, 307-217, 2009.

[187] See, Convention 108, Art. 2.

gal persons, which is, according to it, that the contracting parties may extend personal data protection deals to the legal persons under the national law.
In this regard, the Strasbourg Court provided a clarification. The Strasbourg Court considers that is necessary to protect the data of legal persons based on the right to respect for private and family life, home, and correspondence under Article 8 of the ECHR.[188]

3. The Concept of Personal Data under the APEC Privacy Framework

The APEC Privacy Framework is another non-binding international legal instrument in the field of personal data protection. The APEC Privacy Framework aims to improve the standard of information privacy protection throughout the APEC countries of the Asia-Pacific,[189] and to facilitate the trans-border flow of personal information between those countries.
The APEC Privacy Framework, unlike OECD Privacy Guidelines and Convention 108, regulates "personal information" and not "personal data".
Personal information under the APEC Privacy Framework means "*any information about an identified or identifiable individual*".[190] APEC has chosen to regulate information, not data, as it wants to protect the privacy of the information subject. It specifies that "information" is already the result of data processing, so there is a more immediate violation of individual privacy,[191] thus the need for greater protection. Finally, the APEC Privacy Framework emphasises that the

[188] See, Judgment of the ECtHR, *Bernh Larsen Holding AS and Others v. Norway*, of 14 March 2013.

[189] APEC countries are Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; the Philippines; the Russian Federation; Singapore; Chinese Taipei; Thailand; the United States of America; Vietnam.

[190] See, APEC Privacy Framework, Part II, scope, Article 9.

[191] Ibid., Preamble, Article 1.

framework can only apply to information about living individuals, not to legal persons.[192]

[192] Ibid., page 9.

Chapter 2
The Concept of Personal Data under EU Legal Instruments

1. The Concept of Personal Data under the GDPR

The development of the definition of personal data in the EU law started in 1995 when the EU Institutions enacted the Data Protection Directive (DPD). In 2018, the DPD was replaced by the General Data Protection Regulation (GDPR).
The definition of personal data in the GDPR is essentially the same as that in the former DPD.
The main difference between the two definitions is that the GDPR provides a more extensive yet concise definition, considering developments in technology and communications. Another difference regards the elaboration of the identifiability criterion; Recital 26 of the GDPR states "*To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly*".
The GDPR defines "personal data" as "*any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person*".[193]
According to this definition, any kind of information could be considered personal data; this broad definition of personal data has received criticism from legal scholars.[194]

---

[193] See, GDPR, Article 4.

[194] See, Purtova, pages 50-52.

The terms "identified", and "identifiable natural person" are the key to interpreting this definition. The possibility of matching data processed by the computer to a specific person will depend on various factors, such as their technical capabilities and the type of data.[195]

Legal scholar states that it must satisfy two requirements, to define whether data is personal data or not. The first requirement is called the "relation" requirement, which means the information needs to relate to a natural person. The second requirement is the "identification" requirement, according to it, the natural person must be identified or identifiable from that information.[196]

To derive a concise concept of personal data and facilitate its implementation by the EU Member States, the EU has adopted a non-binding opinion on the concept of personal data issued by the WP29.[197]

2. *The Four Elements of the Concept of Personal Data according to the Opinion of WP29*

According to the WP29 opinion, the definition of personal data consists of four main four elements: *any information*, *relating to*, *an identified or identifiable*, and *natural person.*[198]

First, the term "*any information*" suggests a broad interpretation of the concept of personal data and may fall within the concept of personal data regardless of its nature, content, or format. Under personal data, the nature of information is not important; the information does not matter whether it is true or proven and may include "objective" information, such as names, surnames, and birthdays, and "sub-

---

[195] C. Kuner, *European Data Privacy Law and Online Business*, Oxford University Press, 2003.

[196] See, Wong, page 519.

[197] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, WP 136, of 20 June 2007.

[198] Ibid., pages 6-24.

jective" information, such as opinions or assessments, about individuals, who may be a consumer, patient, employee, etc. As for the content, there are no specific requirements; the information could be about the life of the individual in their life and not just have to be private or family life. Personal data can take any form, such as alphabetical or numerical data, pictures, video, or sound.

In the opinion of the WP29, human tissue samples only represent sources of biometric data which may be subject to separate sets of standards. Human tissue samples are considered personal data only when combined with other additional information or used in a certain technological context.

Under the GDPR, genetic data and biometric data are considered a single category that differs from personal data. Genetic data refers to "*personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question*, and biometric data refers *personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data*".[199]

Second, the term "relating to" means any information that has any connection to an individual can define personal data. In many contexts, the term is interpreted very broadly, and this broad method of interpretation is considered absurd.[200] For a correct interpretation of this term, it is necessary to limit the connection between information and the natural person.

Third, the words "identified or identifiable" concern the identification requirement. Identified means a natural person is distinguished from all other persons or a group, and identifiable means a natural person who has not been identified yet, but the identification is possible. The identification can be directly identified, such

[199] See, GDPR, Article 4, Paragraphs 13-14.

[200] See, Wong, page 519.

as a name with additional information, or indirectly identifiable, which means information allows the individual to be singled out.[201] According to the WP29 opinion, it should be noted that identifiability needs to take into consideration the standard of "*all the means likely reasonably to be used either by the data controllers or processors*". For instance, the costs and time required for the identification process, the technology available at the time of the processing, technological developments, and the purpose of the processing.[202]

Last, the term "natural person" means that the unique beneficiaries of data protection standards under EU legal instruments are only living beings,[203] so the standards of personal data protection are not applied to a deceased person, except when the personal data of a deceased person is also connected to a living individual,[204] or when that personal data is protected by the specific personal data protection rules. In addition, the right to data protection is not applied to legal persons, but legal persons can have protection under the right to respect for private and family life, home, and correspondence of Article 8 of the ECHR,[205] and legal persons can be regulated under national law, according to Convention 108. In addition, the WP29 explains that the protection of unborn children's data depends on national legal systems.

The definition of personal data in the GDPR is like the OECD Privacy Guidelines and Convention 108, as the language of the GDPR is very close to the language of Convention 108. These two legal instruments are considered a cornerstone of the

---

[201] F. J. Z. Borgesius, *Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation*, Computer Law & Security Review 32, 2016, pages 256-271.

[202] P. Voigt, and A. Von Dem Bussche, *The EU General Data Protection Regulation (GDPR) A Pratical Guide*, Springer International Publishing, 2017.

[203] See, GDPR, Article 1.

[204] Ibid., Recital 27.

[205] See, Judgment of the ECtHR, *Bernh Larsen Holding AS and Others v. Norway*, of 14 March 2013.

European framework on the protection of personal data,[206] as they have had an impact on the EU legal instruments on personal data protection.

[206] C. De Terwangne, *Council of Europe convention 108+: A modernized international treaty for the protection of personal data*, Computer Law & Security Review, no. 40, 2021.

Chapter 3
The Concept of Personal Information under Chinese Legal Instruments

In the Chinese legal system, there is no definition of personal data. Chinese legislators have chosen to regulate "Personal Information" since the word "information" (信息（xinxi）in Chinese) has a very long history in China, and the word "data" (数据（shuju）in Chinese), in China, is commonly used in the context of the internet. This means, that in China, data refers to information created on the internet.

The first time to have an explicit definition of personal information in China began in 2017 when the Chinese Cybersecurity Law, [207] and the General Provisions of the Chinese Civil Code came into force.

Even though the explicit definition of personal information in the Chinese context began in 2017, personal information protection has been mentioned in many Chinese laws since 2013, such as the Chinese Law of Protection of Consumer Rights and Interests,[208] Chinese Cybersecurity Law, and Chinese E-Commerce Law.[209]

Currently, there are three definitions of Personal Information in the Chinese legal system: Article 1034 of the Chinese Civil Code, which entered into force on 1

---

[207] Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ (中华人民共和国网络安全法, Chinese Cybersecurity Law), of the 24th Meeting of the Standing Committee of the 12th National People's Congress of the People's Republic of China, of 7 November 2016.

[208] Zhōnghuá rénmín gònghéguó xiāofèi zhě quányì bǎohù fǎ (中华人民共和国消费者权益保护法, Chinese Law of Protection of Consumer Rights and Interests), of the 5th Meeting of the Standing Committee of the 12th National People's Congress of the People's Republic of China, of 25 October 2013, Article 14.

[209] Zhōnghuá rénmín gònghéguó diànzǐ shāngwù fǎ （中华人民共和国电子商务法， Chinese E-Commerce Law）of the 5th Meeting of the Standing Committee of the 13th National People's Congress of the People's Republic of China, of 31 August 2018, Article 5.

January 2021; Article 76, Paragraph 5 of the Chinese Cybersecurity Law, which entered into force on 1 June 2017; and Article 4 of the Chinese Personal Information Protection Law (PIPL), which entered into force on 1 November 2021.

1. *The Concept of Personal Information under the Chinese Civil Code and the Cybersecurity Law*

Personal Information, under Article 1034, Paragraph 2 of the Chinese Civil Code means "*the information recorded electronically or in other ways that can be used, by itself or in combination with other information, to identify a natural person, including the name, date of birth, identification number, biometric information, residential address, telephone number, email address, health information, whereabouts, and the like, of the person.*",[210] and under Article 76, Paragraph 5 of the Cybersecurity Law, personal information is "*all kinds of information recorded in electronic or other forms that can be used independently or in combination with other information to identify a natural person, including but not limited to the natural person's name, date of birth, identity document number, biometric information, address, telephone number, etc.*".[211]

The Chinese Civil Code and the Chinese Cybersecurity Law provide a similar definition of Personal Information. In these definitions, the term "independently" means "directly" or "identified", and the phrase "in combination with other information" refers to the terms "indirectly" or "identifiable".

---

[210] Translated by the , the original text is "个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名，出生日期，身份证件号码，生物识别信息，住址，电话号码，电子邮箱，健康信息，行踪信息等".

[211] Translated by the author, the original text is "个人信息, 是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息, 包括但不限于自然人的姓名, 出生日期, 身份证件号码, 个人生物识别信息, 住址, 电话号码等".

2. *The Concept of Personal Information under the PIPL and the ISTPISS*

The PIPL is the first and main Chinese law on personal information protection. Article 4 of the PIPL states "*Personal Information means all kinds of information recorded in electronic or other forms related to an identified or identifiable natural person, excluding anonymized information*".[212]

The definitions of Personal Information in the Chinese legal system are very similar, but the PIPL definition is more like the GDPR one.

In the Chinese legal system, understanding the concept of personal information is imperative by analysing the Information Security Technology-Personal Information Security Specification (ISTPISS),[213] adopted by the Chinese National Information Security Standardization Technical Committee (TC260) in 2017. The Chinese National Information Security Standardization Technical Committee is a Committee of the National Standard of the People's Republic of China. The ISTPISS contains standards concerning personal information entered into force on 1 May 2018 and was replaced by version 2020,[214] which entered into force on 1

---

[212] Translated by the National People's Congress (NPC), the original text is "个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息".

[213] Zhōnghuá rénmín gònghéguó guójiā shìchǎng jiāndū guǎnlǐ zǒngjú (中华人民共和国国家市场监督管理总局, State Administration for Market Supervision of the People's Republic of China), and Zhōngguó guójiā biāozhǔnhuà guǎnlǐ wěiyuánhuì (中国国家标准化管理委员会, Standardization Administration of the People's Republic of China), Information Security Technology-Personal Information Security Specification, GB/T 35273-2017, of 29 December 2017.

[214] Zhōnghuá rénmín gònghéguó guójiā shìchǎng jiāndū guǎnlǐ zǒngjú (中华人民共和国国家市场监督管理总局, State Administration for Market Supervision of the People's Republic of China), and Zhōngguó guójiā biāozhǔnhuà guǎnlǐ wěiyuánhuì (中国国家标准化管理委员会, Standardization Administration of the People's Republic of China), Information Security Technology-

October 2020. The ISTPISS is regarded as the Chinese National Standard and is issued by the Standardization Administration of the People's Republic of China (SAC),[215] and by the State Administration for Market Supervision of the People's Republic of China (SAMR).[216]

It provides the standards regarding the protection of personal information and a more detailed definition of personal information and sensitive information.[217] According to the ISTPISS, personal information includes thirteen categories: basic personal information,[218] personal identity information,[219] personal biometric information,[220] online identity information,[221] physiological and health information,[222] personal education information,[223] personal property information,[224]

Personal Information Security Specification, GB/T 35273-2020 repealing GB/T 35273-2017, of 6 March 2020.

[215] The SAC is the central administration for setting Chinese national standards organization that undertakes unified management, supervision, and overall coordination of standardization work in China.

[216] The SAMR is an agency of the Chinese government charged with regulating areas such as market competition, monopolies, intellectual property, and drug safety.

[217] C. Wang, *GDPR gèrén shùjù quán yǔ《wǎngluò ānquán fǎ》gèrén xìnxī quán zhī bǐjiào (GDPR 个人数据权与《网络安全法》个人信息权之比较, Comparison of personal data rights under GDPR and personal information rights under the Cybersecurity Law)*, 网络空间张略论坛 Cyberspace Strategy Forum, 2018.

[218] name, date of birth, gender, ethnic group, nationality, family relation, address, personal phone number, email address, etc.

[219] ID card, military officer certificate, passport, driver's license, employee ID, pass, social security card, residence certificate, etc.

[220] personal gene, fingerprint, voice print, palm print, auricle, iris, facial recognition features, etc.

[221] personal information subject's account, IP address, personal digital certificate, etc.

[222] records generated in connection with medical treatment, such as pathological information, hospitalization records, physician's instructions, test reports, surgical and anesthesia records, nursing records, medication administration records, drug, and food allergy, fertility information, medical history, diagnosis, and treatment, family illness history, history of present illness, and history of infectious, and personal health information, such as weight, height, lung capacity, etc.

personal communication information,[225] contact information,[226] personal web surfing record,[227] information of often used equipment,[228] personal location information,[229] and other information.[230]

As it shows, the Chinese legislators have given a very detailed list of what information is considered personal information, so it is a significant difference from the international or the EU legal orders. This also means that in China is considered personal information only the kind of information listed under the ISTPISS, due to the ISTPISS being a binding document. These pieces of information are already listed in the thirteen categories of personal information of the ISTPISS.

---

[223] personal occupation, position, work unit, education background, academic degree, educational experience, work experience, training records, transcripts, etc.

[224] bank account, identification information (password), bank deposit information (including the amount of funds, payment, and collection records, etc.), real estate information, credit records, credit information, transaction, and consumption records, bank statement, etc., and virtual property information such as virtual currency, virtual transactions, and game CD keys.

[225]communication records and content, SMS, MMS, emails, data that describe personal communications (often referred to as metadata), etc.

[226] contacts, friends list, list of chat group, email address list, etc.

[227] records of personal information subject's operations stored in logs, including web browsing records, software use records, click records, favorite lists, etc.

[228] the information describing the general conditions of the equipment often used by an individual, including hardware serial number, equipment MAC address, list of software, and unique equipment identifier (e.g., IMEI/Android ID/IDFA/Open UDID/GUID/SIM card IMSI information, etc.

[229] records of whereabouts, precise location information, accommodation information, longitude, and latitude, etc.

[230] marriage history, religious beliefs, sexual orientation, undisclosed criminal records, etc.

Chapter 4
Approaches or Models used to analyse the Concept of Personal Data (Information)

To understand the concept of personal data, it is also of great importance to know the approaches or models used in the various legal orders and systems, which directly determine whether there is a personal data breach.

The approach or model, in this case, represents the purpose of the enactment of the law, and the concept of personal data should be interpreted following that purpose. In a nutshell, the approach assumes what data protection law aims to protect for an individual.

Under international legal order, the main approach is the "privacy approach". This approach means that the protection of personal data needs to protect the privacy of an individual.

Instead, the EU legal order has adopted its approach called the "content-purpose-result" approach.

Such approaches have significantly influenced the Chinese legal system, which currently applies the dual-dimensional model.

It is explained in detail below.

1. The Privacy Approach

Under international legal order, the right to personal data protection is not recognised as an individual and distinct right. International legal instruments, such as the OECD Privacy Guidelines, Convention 108, and the APEC Privacy Framework, aim to protect the right to privacy of an individual. Therefore, the right to personal data protection is just a sub-right of the right to privacy. For example, one of the reasons that the OECD rejected the suggestion of the OECD Review Working Group to introduce the de-identification technical of personal data dur-

ing the 2013 review work is that the OECD believes that de-identification technical increases the risk of privacy, even though it has benefits on personal data protection.[231]

The right to privacy, also known as the right to respect for private life, emerged in international human rights law in the Universal Declaration of Human Rights (UDHR), in ECHR, and is enshrined in EU law in the EU Charter of Fundamental Rights (CFR or EU Charter). It is the right to have a general prohibition of interference and protection of the public interest.[232] Instead, the right to personal data protection is modern and active, needing to balance interests between public and individual interests and protect individual interests.[233]

The "privacy" approach means that the evaluation of a possible personal data protection breach must be made from the point of view of privacy protection. This approach is still the main approach applied in the international legal system in the field of personal data protection.[234] Actually, the Strasburg Court applied under Article 8 of the ECHR, which affirms the right to respect private and family life, home, and correspondence in the case of the violation of Convention 108.[235] This

---

[231] See, Part 2, Chapter 6; see also, OECD, *Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines*, pages 10-11.

[232] Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights, Handbook on European data protection law: 2018 edition, Publications Office, 2019, pages 18-21.

[233] See, Judgment of the CJEU, of 9 November 2010, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, joined cases C-92/09 and C-93/02, ECLI:EU:C:2010:662; See also, Opinion of Advocate General Sharpston, delivered on 17 June 2010, described the case as involving two separate rights: the "classic" right to the protection of privacy and a more "modern" right, the right to data protection.

[234] See, Judgment of the ECtHR, *M.L., and W.W. v. GERMANY*, of 28 June 2018; Judgment of the ECtHR, *Vučina v. Croatia*, of 24 September 2019.

[235] See, Judgment of the ECtHR, of Grand Chamber, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, no. 931/13, of 27 June 2017; Judgment of the ECtHR, *Z v. Finland*, of 25 February 1997.

means whether an individual would like to protect their right to data protection shall apply under the right to respect private life.[236] As a result, whether there is a personal data breach, there must be a breach of the right to respect for private life, otherwise, it cannot find its jurisdiction in international courts. Also, it means that whether personal data is processed, but the data processing has not evaded the sphere of individual privacy, the data controller or data processor may not be called responsible under international law. This approach was also applied in the context of EU law, but since the DPD came into force, the privacy approach has gradually been replaced by the "content-purpose-result".[237]

Since international legal instruments do not recognise the right to data protection and use the privacy approach, legal scholars misunderstand that the right to privacy and the right to personal data protection are identical rights.[238] Other legal scholars say the right to privacy and the right to personal data protection are related in many situations, they are certainly two distinct rights.[239]

2. The Content-Purpose-Result Approach

The WP29 developed the "content-purpose-result" approach and replaced the "privacy" approach. [240] According to the WP29 opinion, whether data can relate to an individual depends on one of three elements: content, purpose, or result. There-

---

[236] Council of Europe, European Court of Human Rights, *Guide to the Case-Law of the European Court of Human Rights-Data protection*, 2021.

[237] See, Wong, pages 517-532; and See, Judgment of the CJEU, of 17 July 2014, *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S,* joined cases C-141/12, and C-373/12, ECLI:EU:C:2014:2081.

[238] M. Tzanou, *Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right*, International Data Privacy Law, Vol. 3, No. 2, 2013.

[239] J. Kokott, and C. Sobotta, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, International Data Privacy Law, Vol. 3, No. 4, 2013.

[240] See, W29, *Opinion 4/2007 on the concept of personal data*, pages 9-12.

fore, data can only be defined as personal data when it conforms to one of these three elements.

Firstly, the "content" element means information must be about a particular person, no matter the purpose of the data controller or a third party. Secondly, the "purpose" element indicates that all the circumstances surrounding the specific case must be taken into consideration. Finally, the "result" element points out that data is considered personal data when the use of the specific data has an impact on a certain person's rights and interests.

Today, the "content-purpose-result" approach has fully been applied to the CJEU cases.[241]

The EU legal order differs from the international legal order; there is a clear distinction between the right to privacy and the right to personal data protection. The right to privacy is recognised under Article 7 of the Charter of Fundamental Rights of the European Union (EU CFR), and the right to personal data protection is contained in Article 8 of the EU CFR.

At this juncture, it is necessary to underline that the obligations to privacy and personal data protection do not directly result from Articles 7 or 8 of the EU CFR but from the GDPR. According to Article 51 of the EU CFR, its provisions address the institutions, bodies, offices, and agencies of the Union and the Member States when implementing EU law. Under this interpretation, the rights to privacy and personal data protection appear not to directly create obligations for private parties.

In addition, the distinction between the right to privacy and the right to personal data protection is not only theoretical but also applied in Court of Justice of the European Union (CJEU) cases.[242]

---

[241] See, Judgment of the CJEU, of 20 December 2017, *Peter Nowak v Data Protection Commissioner,* C-434/16, ECLI:EU:C:2017:994.

[242] See, Judgment of the CJEU, of Grand Chamber, of 13 May 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, case C-131/12, ECLI:EU:C:2014:317.

Furthermore, it is necessary to make the distinction between the right to privacy and the right to data protection for the purposes of applying the rights recognised in the GDPR to data subjects.

3. The One-Dimensional Model and the Dual-Dimensional Model

Before the Chinese Cybersecurity Law and the General Provisions of the Chinese Civil Code came into force in 2017, the Chinese legal system used the "one-dimensional" model (一元制 (yiyuanzhi) in Chinese) to evaluate whether there was a personal information breach or not. The one-dimensional model means personal information protection is considered part of the right to privacy. It is the same "privacy" approach that has been applied in the international legal order.

After 2017, the Chinese legal system recognises the right to privacy and the right to personal information protection as two individuals and autonomous rights, like in the EU legal order. The one-dimensional model has been replaced by the "dual-dimensional" model (二元制 (eryuanzhi) in Chinese).[243]

The dual-dimensional model is like the "content-purpose-result" approach adopted in the EU legal order. It means that the right to privacy and the right to personal information protection are two equal rights.

Today, the right to personal information protection is also directly mentioned under Articles 111 and 1034 of the Chinese Civil Code and Article 2 of the PIPL, and the dual-dimensional model is transplanted into the Personal Information Protection Law, the Chinese Civil Code, and in the Chinese Courts.

---

[243] Y. Li, The Research on the "Dual System" Protection and Claim Basis of the Personal Privacy and Information in The General Principles of Civil Law (论« 民法总则» 中个人隐私与信息的 "二元制" 保护及请求权基础), Journal of Zhejiang Gongshang University, No. 3 General no. 144, 2017.

In recent cases, *Huang X v. Tencent Technology (Shenzhen) Co., Ltd.*,[244] and *Ling XX v. Beijing Weibo Shijie Technology Co., Ltd.*,[245] the Chinese judges state that the right to privacy and the right to personal information protection are two individual civil rights that are complementary to each other.

[244] See, Judgment of case *Huáng mǒu sù téngxùn kējì (shēnzhèn) yǒuxiàn gōngsī, téngxùn kējì (běijīng) yǒuxiàn gōngsī děng yǐnsī quán, gèrén xìnxī bǎohù jiūfēn àn (黄某诉腾讯科技(深圳)有限公司、腾讯科技(北京)有限公司等隐私权、个人信息保护纠纷案, Huang X v. Tencent Technology (Shenzhen) Co., Ltd)*, 2019 Jīng 0491 mín chū 16142 hào (2019 京 0491 民初 16142 号, 2019 Jing 0491 Min Chu no.16142), of 30 July 2020.

[245] See, Judgment of case *Líng mǒu mǒu sù běijīng wēi bō shìjiè kējì yǒuxiàn gōngsī yǐnsī quán, gèrén xìnxī quányì wǎngluò qīnquán zérèn jiūfēn àn (凌某某诉北京微播视界科技有限公司隐私权、个人信息权益网络侵权责任纠纷案，Ling XX v. Beijing Weibo Shijie Technology Co., Ltd)*, 2019 Jīng 0491 mín chū 6694 hào (2019 京 0491 民初 6694 号，2019 Jing 0491 Min Chu no. 6694), of 30 July 2020.

Chapter 5
The Concept of Special Category of Data

Personal data differs from sensitive data. Sensitive data is recognised as a special category of data. Such data are subject to additional protection compared to personal data.

1. The Concept of Sensitive Data under Convention 108

Article 6 of Convention 108, as originally adopted, stated, "*Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions*". In Convention 108+, there is a reformulation of Article 6, which now reads thus: "1. *The processing of genetic data; personal data relating to offences, criminal proceedings and convictions, and related security measures; biometric data uniquely identifying a person; personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention. 2. Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination*".
Convention 108 was highly influential in the adoption of provisions on sensitive data in the EU law, as well as in the DPD.[246] Article 8 DPD regulated the processing of special categories of data, now replaced under Article 9 of the GDPR.

[246] L. Georgieva and C. Kuner, *Article 9. Processing of special categories of personal data in the EU General Data Protection Regulation (GDPR)*, Oxford University Press, 2020.

2. *The Concept of Sensitive Data under the GDPR*

Indeed, Article 9 of the GDPR grants special protections to personal data revealing *"racial or ethnic origin, personal data revealing political opinions, religious or other beliefs, including philosophical beliefs, personal data revealing trade union membership, genetic data, and biometric data processed for the purpose of identifying a person, and personal data concerning health, sexual life, or sexual orientation*, these data are also known as sensitive data. Under Article 9 of the GDPR, such data may generally not be processed, except under certain provided circumstances, such as (1) when the data subject has given his explicit consent, except the EU or Member State law prohibits it, (2) processing by the data controller for employment purposes, (3) when processing is necessary to protect "*the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent*", (4) processing is carried out by non-profit bodies in the course of their legitimate activities, (5) when "*the processing relates to personal data, which are manifestly made public by the data subject*", (6) processing is necessary for judicial purposes, (7) processing is necessary for public interest, (8) processing is necessary for "*the purposes of preventive or occupational medical, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards*", (9) processing is necessary for public, (10) processing is necessary for public interest, scientific or historical purposes. It should be noted that fulfilling these exceptions does not exclude personal data from protection under the GDPR, but rather from the additional protection of Article 9.

The WP29 issued several opinions and papers concerning the processing of sensitive data, including general issues of sensitive data,[247] or specific topic papers, such as biometric data,[248] and genetic data.[249]

Article 9 of the GDPR unlike Convention 108+ does not mention personal data relating to offences, criminal proceedings and convictions, and related security measures, yet Article 10 of the GDPR states "*Personal Data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of the official authority*".

The list of sensitive data stated in Article 9 of the GDPR is exhaustive, so it is not possible to add new categories of sensitive data.

Racial or ethnic origin refers to information such as minority affiliation and skin colour. Political opinions can include such things as affiliation with a political party, participation in demonstrations, and political statements or publications. Religious or philosophical beliefs refer to membership in a religious confession or in an organisation that focuses on a philosophical belief. Trade union membership concerns information documenting such membership. A natural person's sex life

---

[247] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, WP187, of 13 July 2011.

[248] Article 29 Data Protection Working Party, *Working document on biometrics*, WP80, of 1 August 2003; Article 29 Data Protection Working Party, *Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)*, WP96, of 11 August 2004; Article 29 Data Protection Working Party, *Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, WP112, of 30 September 2005, and Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies*, WP193, of 27 April 2012.

[249] Article 29 Data Protection Working Party, *Working Document on Genetic Data*, WP91, of 17 March 2004.

or sexual orientation includes information about whether an individual is heterosexual, homosexual, bisexual, or of some other orientation, as well as information about sexual practices. For instance, the consumption of pornography. In addition, sexual life means details on marital status and intimate personal details. For example, the information concerns gender change.

The CJEU expressly clarified that the category of sensitive data includes not only the data provided directly by the interested party themselves but also all the information that can be deduced and detected from those data, whether it does not correspond to the truth, since it is, in any case, capable of processing information referable to a specific individual. In addition, although the GDPR states exceptions to the prohibition of processing sensitive data, the data controller must always respect the principle of proportionality. This is an extremely important judgement of the CJEU on Article 9 of the GDPR.[250]

3. The Concept of Sensitive Information under the PIPL

On the Chinese side, in the same situation of personal information, legislators chose to use the term "sensitive information" rather than sensitive data.

Article 28 of the PIPL defines sensitive personal information, which means "*personal information that once leaked or illegally used, may easily lead to the infringement of the personal dignity of a natural person or may endanger his personal safety or property, including information such as biometrics, religious belief, specific identity, medical health status, financial accounts, and the person's whereabouts, as well as the personal information of a minor under the age of 14*

[250] See, Judgment of the CJEU, of Grand Chamber, of 1 August 2022, *Vyriausioji tarnybinės etikos komisija*, case C-184/20, ECLI:EU:C:2022:601.

years".[251] In addition, all personal information concerning minors under the age of 14 is considered sensitive information, which means personal information under the age of 14 has additional protection. Indeed, in China, the processing of sensitive information is possible only when it has a specific purpose and sufficient necessity and is protected by strict protective measures. Furthermore, Article 29 of the PIPL states that to process sensitive information, the information handler must obtain the separate consent of the personal information subject.[252]

An exhaustive and mandatory list specifying sensitive information is contained within the ISTPISS.[253] According to it, sensitive information in China includes five categories: personal property information,[254] physiological and health information,[255] personal biometric information,[256] personal identity information,[257] and

[251] Translated by the National People's Congress (NPC), the original text is "敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息".

[252] See, Part 2, Chapter 3, Paragraph 2.

[253] See, ISTPISS, GB/T 35273-2017, Annex B.

[254] bank account, authentication information (password), bank deposit information (including the amount of funds, payment, and collection records), real estate information, credit records, credit information, transaction and consumption records, bank statement, etc., and virtual property information such as virtual currency, virtual transaction, and game CD Keys.

[255] the records generated in connection with medical treatment, including pathological information, hospitalization records, physician's instructions, test reports, surgical and anesthesia records, nursing records, medicine administration records, drug and food allergy, fertility information, medical history, diagnosis, and treatment, family illness history, history of present illness, history of infection.

[256] personal gene, fingerprint, voice print, palm print, auricle, iris, facial recognition features, etc.

[257] ID card, military officer certificate, passport, driver's license, employee ID, social security card, resident certificate, etc.

other information.[258] To be more precise, within this categorization, personal financial information is also regarded as sensitive personal information.

In short, in China, the distinction between personal information and sensitive information depends on the result of its use or the consequence that it could cause the personal information subject to its use.[259]

[258]Sexual orientation, marriage history, religious preference, undisclosed criminal records, communications records and content, contacts, friends list, list of chat groups, records of whereabouts, web browsing history, precise location information, accommodation information, etc.

[259] See, ISTPISS, GB/T 35273-2017.

Chapter 6
Anonymisation and Pseudonymisation Techniques under International, EU, and Chinese Legal Instruments

Not all legal instruments analysed up to now recognise anonymisation and pseudonymisation data.

Anonymisation is the technical process of removing personal data to achieve irreversible prevention of the identification of individuals. It is a way of modifying personal data so that the individual is no longer identifiable.[260] Pseudonymisation is a technical of deidentification, which means when data is no longer attributable to a specific individual without the use of additional information, or personal data is replaced by a pseudonym.[261]

Pseudonymisation and anonymisation are techniques excluded in the OECD Privacy Guidelines, as the OECD states that they increase the risk to an individual's privacy in the event of "re-anonymisation".[262] For instance, in health research, collecting anonymised data is not necessary to obtain the consent of the data subject, but if such data is re-anonymised to process it, this could pose challenges around obtaining consent.

To date, only the GDPR and the PILL recognise anonymous and pseudonymous data (information) and have given the concept. However, the Explanatory Report of Modernized Convention 108 affirmed "*Data is to be considered as anonymous only as long as it is impossible to re-identify the data subject or if such re-identification would require unreasonable time, effort or resources, taking into consideration the available technology at the time of the processing and techno-*

[260] See, GDPR, Recital 26.

[261] Ireland Data Protection Commission, *Guidance Note: Guidance on Anonymisation and Pseudonimisation*, 2019.

[262] Organisation for Economic Cooperation and Development, Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, on 11 July 2013.

logical developments", and pseudonymous data "*is thus to be considered as personal data and is covered by the provisions of the Convention*".

The current technology recognises several anonymisation techniques, but all techniques can be divided into two categories: randomization and generalization.[263] Randomization consists of the accuracy of data by removing the strong link between the data and the individual.[264] Generalization is about generalizing or diluting the respective scale or order of the data.[265] For example, write a city rather than a region, a day rather than a week.

1. Anonymisation and Pseudonymisation Techniques under the GDPR

The EU legal order recognises anonymisation and pseudonymisation techniques under the GDRP. The EU requires very high standards for anonymised data, so the GDPR states that the personal data protection standards do not apply to anonymised data, and underlines that if the personal data controller or processor can restore the anonymous data, the personal data will be subject to the GDPR.[266]

According to the EU data protection legislators, anonymisation has several benefits for the personal data controller or processor, considering anonymised data does not have to comply with the data protection obligation.[267] In this way, personal data controllers and processors can save time, money, and staff resources.[268] The GDPR also states that pseudonymisation is a perfect technical measure to ensure personal data security.[269]

---

[263] See, P. Voigt, and A. Von Dem Bussche, pages 28-33.

[264] Article 29 Data Protection Working Party, *Opinion 5/2014 on Anonymisation Techniques*, WP 216, of 10 April 2014.

[265] See, WP29, Opinion 5/2014, pages 13-19.

[266] See, GDPR, recital 26.

[267] Ibid.

[268] See, P. Voigt, and A. Von Dem Bussche, pages 29-30.

[269] See, GDPR, Recital 28.

Article 4, Paragraph 5 of the GDPR provides a clear definition of pseudonymisation, which means "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*".

Before the GDPR entered into force in the EU legal order, the concept of "pseudonymisation" had been used in policy discourses concerning data protection,[270] so it is a term adopted recently.

Under the GDPR, treating personal data as pseudonymized personal data requires two cumulative conditions to be met. First, personal data must go through a process that renders it unlinkable to a specific data subject without the use of additional information. Second, the additional information that allows identification of the individual must be kept separately.[271]

The anonymisation technique eliminates the connection with the individual, and pseudonymized data focuses on reducing contestability between personal data and the natural person.[272] According to the GDPR, Recital 29 pseudonymised data is considered identifiable data, and it is subject to the GDPR and other data protection measures.

The possibilities of re-identification have considerably increased due to technological progress and the more widespread circulation of data. Therefore, the notion of anonymous data and pseudonymized data has been the subject of new reflections. Recently, the CJEU provided a new perspective on the analysis and in-

---

[270] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Anonymity on the Internet*, WP6, of 3 December 1997; Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, WP261, of 10 April 2014.

[271] See, GDPR, Article 4, Paragraph 5.

[272] S.Y. Esayas, *The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach*, European Journal of Law and Technology, Vol 6, No 2, 2015.

terpretation of the re-identification risk assessment in Case T-557/20.[273] According to the latter case, the CJEU states that "*in order to assess whether data are anonymous or pseudonymous, it is necessary to consider whether there is any 'additional information' that can be used to attribute the data to specific data subjects*". This means that to establish whether the information constitutes personal data, it is necessary to look from the point of view of the recipient of the same and evaluate whether the possibility of combining the information transmitted with any additional information held by the third party constitutes a reasonably feasible means of identifying the data subjects.

2. Anonymisation and Pseudonymisation Tecniques under the PIPL and the ISTPISS

On the Chinese side, Article 4 of the PIPIL states that anonymised information is not considered personal information, so it is not subject to regulation under the PIPIL. Therefore, the situation is highly similar with respect to the EU Law, the difference consists in the pseudonymised data. Chinese legislators adopted a broader concept of pseudonymisation. To be precise, Chinese legislators chose to use the term "de-identification" rather than "pseudonymisation". According to Article 3.5 of the ISTPISS, "de-identification" means it is not possible to identify the information subject without using other information or relative information and includes pseudonyms, encryption, hash functions and other technical means to replace the personal identifiers.

Even though pseudonymisation data is regulated by the data proception law, it can also help the data controller or processor to reduce the danger of identification or harm from a data breach.[274]

---

[273] See, Judgment of the CJEU, of 26 April 2023, *Single Resolution Board v European Data Protection Supervisor*, Case T-557/20, ECLI:EU:T:2023:219.

[274] See, GDPR, Article 32.

Conclusion of Part 2

The purpose of this Part was to determine the concept of personal data under international and EU legal instruments and the concept of personal information under Chinese legal instruments.

The definitions of personal data contained in international, and EU legal instruments are completely the same and reflect the intention of lawmakers to have a broad and general concept. [275] In fact, knowing the concept of personal data, which is not a simple definition but a detailed and precise notion, is often hard.[276]

In the EU, there is an individual and distinct constitutional right to personal data protection, which does not exist in the international arena, as under international legal order, personal data protection can only be enforced under the right to privacy, the so-called privacy approach.

The concept of personal information in the Chinese legal system is more like that of the EU, also in terms of application.

However, there is a right to personal data (information) protection in the EU legal order and in the Chinese legal system, but their natures are different. In the EU, the right to personal data protection is a constitutional right. The right to personal information in China is a civil right with a constitutional basis under Article 38 of the Chinese Constitution,[277] as is the right to privacy. In China, the right to priva-

---

[275] Council of EU, Common Position (EC) No 1/95, adopted by the Council on 20 February 1995, with a view to adopting Directive 95/…/EC of the European Parliament and of the Council of … on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J.E.C. No C 93/1, of 13 April 1995.

[276] B. Schneier, *Why Anonymous Data Sometimes Isn't*, Wired, 12 December 2007.

[277] Article 38 of the Constitution of the People's Republic of China: The personal dignity of citizens of the People's Republic of China is inviolable. Insult, libel, false accusation, or false incrimination directed against citizens by any means is prohibited.

cy and the right to personal information protection are considered part of personal dignity.[278]

The legal scholar states "information" is composed of "data" plus "meaning",[279] but the meaning of the personal "information" contained in the PIPL has the same meaning as the meaning of personal "data" contained in international and EU legal instruments.

The reason that the Chinese legislators adopted the term "information" instead of "data", is due to Chinese legal history and customs,[280] as in the Chinese language "data" is information in electronic format. It should also be noted that, in the Chinese legal system, there is a legal definition of data. According to Article 3 of the Chinese Data Security Law, data means "*any record of information electronically or otherwise*".[281]

Regarding the concept of sensitive data (information), the concepts contained in international, EU, and Chinese legal instruments are similar.

They recognise sensitive data as a special category with more restrictive rules than personal data (information). Only the GDRP states that it is forbidden to process sensitive data except in the situations provided for by the regulation itself.

Sensitive data (information) are only those listed by the law, but international and Chinese legal instruments give some flexibility. For instance, in the Chinese legal system, information leaked or illegally used that may easily cause grave harm to dignity can be classified as sensitive information. Furthermore, in accordance with the ISTPISS list, which carries binding authority within the Chinese legal system, personal financial information is also classified as sensitive information. Con-

---

[278] X. Wang, and C. Peng, *Gèrén xìnxī bǎohù fǎlǜ tǐxì de xiànfǎ jīchǔ (个人信息保护法律体系的宪法基础, The Constitutional Basis of the Personal Information Protection Legal System)*, Tsinghua University Law Journal, Vol. 15, No. 3, 2021.

[279] See, Purtova, pages 50-53.

[280] F. Gao, *The protection of individuals with regard to processing of personal information-On orientation of "Personal Information Protection Act"*, Academic Monthly (2), 2021.

[281] Translated by the author, the original text is "是指任何以电子或者其他方式对信息的记录".

versely, under international and EU legal frameworks, sensitive data is narrowly defined to include the most personal information, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health-related information, and data concerning a person's sex life or sexual orientation, that has the potential to reveal the identity of an individual.

Other two differences: first, in the Chinese legal system, information regarding a minor under the age of 14 is considered automatically sensitive information; second, biometrical and genetic data are considered subcategories of sensitive information.

After the GDPR entered into force, the EU legal order introduced the first legal definition of pseudonymisation. The situation is the same in the Chinese legal system, but the Chinese legislators adopted the word “de-identification” rather than “pseudonymisation”, as they believe that de-identification has a broader meaning.

In both EU law and the Chinese system, anonymous data is not subject to data protection regulations.

There is a lack of regulation in the international legal order regarding anonymisation and pseudonymisation techniques.

PART 3
THE CONSENT OF NETIZENS TO DATA PROCESSING

The rules of personal data processing are dictated by law; personal data processing activities must only be lawful. The consent of the data subject constitutes a basis for lawful personal data processing. Indeed, personal data processing without the data subject's consent or not permitted by law is prohibited. It means the data processor or controller shall obtain direct permission from the data subject before processing their data. The consent of the data subject to data processing represents "information self-determination".[282] Given the importance of the consent of the data subject in personal data processing, it is essential to know how different jurisdictions regulate it. To be specific, when it comes to transborder flows of personal data, there may be situations where it is not clear when consent is considered valid. This problem could cause legal uncertainty, mainly in the infosphere,[283] which has no real border. Today, legal uncertainty in this matter is not noticeable between the legal systems of EU member states owing to the entry into force of the General Data Protection Regulation (GDPR), but instead at an international level, the standards in this regard are very limited, and in the Chinese legal system, it is a matter of recent introduction. In addition to knowing what the rules on the consent of the data subject are like, there is another interesting and important question: Is the consent of the data subject an obligation or a freedom? There are online situations in which it is necessary to give consent to the processing of personal data to access a certain service; if the data subject

[282] L. A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer law international, 2002, pages 150-154.

[283] L. Floridi, *Pensare l'infospera*, Raffaello Cortina Editore, 2020.

refuses to give their consent to data processing, they will be excluded from the service, the so-called*, bundling or tying.*

International, EU, and Chinese legal standards provide different and specific rules regarding the requirements to define valid consent of the data subject and divide between the consent of personal data and the consent of sensitive data, which has more severe restrictions.

This Part explains the concept and rules of data subject consent under International, EU, and Chinese legal instruments and seeks to interpret the value of the consent of the data subject, especially in the context of "bundling". The Part is divided into three Chapters: the first Chapter shows the standards of data subject consent in the international legal order; the following Chapter explains the data subject consent rules under the EU legal order; and the last Chapter describes the data subject consent provisions in the Chinese legal system. It will conclude with a comparative analysis of the consent under international, EU, and Chinese legal instruments. The Part also takes into consideration the case law in this regard, where it is possible.

Chapter 1
The Consent of Data Subject to Data Processing under International Legal Instruments

1. The Consent of Data Subjects under Convention 108

Convention 108 does not define the term "consent" for data processing; it is also absent in the modernised version, but the modernised Convention states that "*data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law*".[284]

A specific and detailed clarification of the term "consent" is contained in the Explanatory Report to the Modernised Convention, which states, "*The data subject's consent must be freely given, specific, informed and unambiguous. Such consent must represent the free expression of an intentional choice, given either by a statement (which can be written, including by electronic means, or oral) or by a clear affirmative action which clearly indicates in this specific context the acceptance of the proposed processing of personal data. Mere silence, inactivity or pre-validated forms or boxes should not, therefore, constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes (in the case of multiple purposes, consent should be given for each different purpose). There may be cases with different consent decisions (e.g., where the nature of the data is different even if the purpose is the same – such as health data versus location data: in such cases, the data subject may consent to the processing of his or her location data but not to the processing of the health data). The data subject must be informed of the implications of his or her decision (what*

[284] Council of Europe, *Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data*, of 128th Session of the Committee of Ministers, of 18 May 2018, Article 5, Paragraph 2.

the fact of consenting entails and the extent to which consent is given). No undue influence or pressure (which can be of an economic or other nature) whether direct or indirect, may be exercised on the data subject and consent should not be regarded as freely given where the data subject has no genuine or free choice or is unable to refuse or withdraw consent without prejudice".[285] This clarification confirms that the term "consent" in modernised Convention 108 has the same meaning of the term "consent" contained under GDPR and affirms the prohibition of bundling, as the consent is to be considered invalid.[286]

The Modernised Convention also mentions consent in two other contexts: transborder flows of personal data and cooperation between supervisory authorities. In the first context, the Modernised Convention makes clear that transfer of personal data is possible when "*the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards*",[287] and in the second context, it affirms that in the case of cooperation between supervisory authorities, the exchange of personal data is possible only when "*such data are essential for cooperation, or where the data subject concerned has given explicit, specific, free and informed consent to its provision*".[288]

2. *The Consent of Data Subjects under OECD Privacy Guidelines and the APEC Privacy Framework*

The definition of the term "consent" is also not included in either the original and revised OECD Privacy Guidelines or the APEC Privacy Framework, but both make limited use of the concept of consent within their collection limitation prin-

---

[285] Council of Europe, Council of Europe Treaty Series - No. 223, *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, of 10 October 2018, Paragraph 42.

[286] See, Part 3, Chapter 2, Paragraph 2.

[287] See, Modernised Convention, Article 14, Paragraph 4, letter a.

[288] Ibid., Article 17, Paragraph 2.

ciple and use limitation principle. In addition, the APEC Privacy Framework also mentions it within the accountability principle.

According to OECD Privacy Guidelines, the collection of personal data should "*be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject*",[289] and personal data may only be disclosed with the consent of the data subject or by the authority of law.[290] Instead, the APEC Privacy Framework states that "*the collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned*",[291] and "*personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except with the consent of the individual whose personal information is collected*".[292] Furthermore, the APEC Privacy Framework underlines that "*when personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence*".[293]

Even though the international legal standards do not have an explicit and direct definition of the consent of the data subject, the Strasbourg Court recognises the importance of obtaining the data subject's prior consent to the disclosure or transfer of their data. The Court declares that in the case of disclosure of personal information without the consent of the data subject, there is a violation of the right to respect for private and family life, home, and correspondence under Article 8 of the European Convention on Human Rights. In the *Radu v. the Republic of Mol-*

[289] See, OECD Privacy Guidelines, 2013, Article 7.

[290] Ibid., Article 10.

[291] See, APEC Privacy Framework, Article 24.

[292] Ibid., Article 25, letter a.

[293] Ibid., Article 32.

dova case,[294] the Court notes that "*a doctor would not be entitled to disclose information of a personal nature even to the applicant's employer without her consent*",[295] and that "*there has been a violation of Article 8 of the Convention in respect of the applicant's right to respect for her private life*".[296] Moreover, the Court explains that the consent of the data subject must be informed and unequivocal to obtain valid consent, citing the case law of *M.S. v. Sweden*,[297] and *Konovalova v. Russia*.[298]

[294] See, Judgment of the ECtHR, *Radu v. the Republic of Moldova*, no. 50073/07, of 15 April 2014.

[295] Ibid., Paragraph 30.

[296] Ibid., Paragraph 32.

[297] See, Judgment of the ECtHR, *M.S. v. Sweden*, no. 20837/92, of 27 August 1997, Paragraph 32.

[298] See, Judgment of the ECtHR*, Konovalova v. Russia*, no. 37873/04, of 9 October 2014, paras 47 and 48.

Chapter 2
The Consent of Data Subject to Data Processing under EU Legal Instruments

The legitimate basis of the consent of the data subject for personal data processing is recognised under the Charter of Fundamental Rights of the European Union (CFR), particularly in Article 8, Paragraph 2, which states "*such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified*".

The legal framework relating to the consent of the data subject contained in the EU legal order is much more advanced than the standards of the international legal order on this matter. The definition of the consent of the data subject was expected from the very beginning of the legislation concerning the protection of personal data with the adoption of the DPD in 1995. According to the DPD, the consent of the data subject means "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*".[299] During the preparatory work of the DPD, the drafters stated that the consent of the data subject had to be "*expressly given*" and "*specific*" and only for sensitive data must it be "*express and written*".[300] Subsequently, the terms "*expressly given*" and "*specific*" are replaced with the terms "*freely given*" and "*specific*" on an amended proposal from the EU Commis-

[299] See, DPD, Article 2, letter h.

[300] COM (90) final, SYN 287, *Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data*, of 13 September 1990.

sion.[301] The definition of the consent of the data subject under the DPD is very close to the concept of the data subject contained in the GDPR, and it had some legal uncertainty,[302] which were whether the consent of the data subject may be presumed, the so-called passive consent, the amount of information required to consent to be informed, and what requirements an explicit consent shall have. Indeed, the EU Commission declares its intention to clarify and strengthen the rules on consent,[303] trying to solve these problems.

The definitions contained in the DPD and the GDPR are similar but not the same. There are two differences: the first is the unambiguous requirement, and the second is that under the definition of the GDPR, consent should be made "*by a statement or by a clear affirmative action*". The unambiguous requirement was also required in the DPD, but only in two contexts. The first, "*personal data may be processed only if the data subject has unambiguously given his consent*",[304] and the last, Member States shall transfer personal data to a third country "*on condition that the data subject has given his consent unambiguously to the proposed transfer*".[305]

1. The Consent of the Data Subject under the GDPR

The consent of the data subject under the GDPR is "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or*

---

[301] COM (92) final, SYN 287, *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data an on the free movement of such data*, of 15 October 1992.

[302] E. Kosta, *Consent in European Data Protection Law*, Martinus Nijhoff Publishers, 2013.

[303] COM(2010) 609 final, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union*, of 4 November 2010, page 9.

[304] See, DPD, Article 7, letter a.

[305] Ibid., Article 26, Paragraph 1.

she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".[306] From this definition, it can be inferred that a valid data subject's consent must satisfy four key criteria. The four elements are free consent or free given, specific, informed, and unambiguous indication.[307]

a) The Criterion of Free Consent or Free Given

"*Free consent*" or "*free given*" means the free expression of an intentional choice. It represents that the data subject has the autonomy to choose whether to give consent to data processing.

According to WP29, the concept of free consent is the possibility for the data subject to exercise their real choice without deception, intimidation, coercion, or other significant negative consequences arising from the lack of consent. It can refuse or withdraw consent,[308] and underlines that "*if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid*".[309]

The GDPR states that before the data subject gives consent, "*the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended*".[310] In addition, the GPDR explains, "*In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case*

[306] See, GDPR, Article 4, Paragraph 11

[307] European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, Version 1.1, of 4 May 2020.

[308] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, WP 187, of 12 July 2011.

[309] Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679*, WP259 rev.01, of 10 April 2018.

[310] See, GDPR, Recital 42.

where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance".[311]

The situation of imbalance is often found in the workplace, between employer and employee,[312] in the context of clinical trials,[313] and is also found in the relationship between online providers and netizens; the latter situation creates the so-called situation of "bundling", which is prohibited. The situation of "bundling" and its relevant case law will be better explained later.

Free consent is also an argument that has interested the CJEU, which states through the case of *Pfeiffer v Deutsches Rotes Kreuz*,[314] that "*the worker must be regarded as the weaker party to the employment contract and it is therefore necessary to prevent the employer being in a position to disregard the intentions of the other party to the contract or to impose on that party a restriction of his rights without him having expressly given his consent in that regard*".[315] Although the case is in the employment context, it can be understood from this conclusion that the orientation of the CJEU is compatible with the opinion of the WP29.

---

[311] Ibid., Recital 43.

[312] Article 29 Data Protection Working Party, *Opinion 2/2017 on data processing at work*, WP 249, of 8 June 2017, pages 21 and 22.

[313] European Data Protection Board, *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b)*, of 23 January 2019.

[314] See, Judgment of the CJEU, of 5 October 2004, *Pfeiffer v Deutsches Rotes Kreuz,* In Joined Cases C-397/01 to C-403/01, ECLI:EU:C:2004:584.

[315] Ibid., Paragraph 82.

The WP29, generally, declares that it is considered free consent only when the data subject has no negative consequences for not giving consent.[316]
Furthermore, the WP29 explains that the data controller must obtain the consent of the data subject by providing information using an easily understood language to the data subject; particularly, it states the information must be "*in a clear and understandable manner, accurate and full information of all relevant issues…such as the nature of the data processed, purposes of the processing, the recipients of possible and the rights of the data subject*".[317]
When the EDPB replaced the WP29, these affirmations of the WP29 were confirmed by the EDPB statements.[318] It underlines, "*When seeking consent, controllers should ensure that they use clear and plain language in all cases. This means a message should be easily understandable for the average person and not only for lawyers. Controllers cannot use long privacy policies that are difficult to understand or statements full of legal jargon. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form. This requirement essentially means that information relevant for making informed decisions on whether or not to consent may not be hidden in general terms and conditions*".[319]

b) The Criterion of Specification

Another requirement to have valid consent is the criterion of specification, which ensures user control and transparency for the data subject.

---

[316] See, WP259 rev.01, pages 6 and 7.

[317] Article 29 Data Protection Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, WP 131, of 15 February 2007.

[318] See, EDPB, Guidelines 05/2020.

[319] Ibid., Paragraph 67.

According to the GDPR, "*the data subject has given consent to the processing of his or her personal data for one or more specific purposes*".[320] It means that the data controller must provide the specific purpose of the consent to the data subject; general consent to data processing is not considered valid, and it is needed to provide the possibility of giving separate consent for different data processing operations.[321] For instance, a netizen registers on a website to enjoy a certain service and consents to the processing of his data in relation to the use of his email to receive updates on this service. If the data controller, in this case, the owner of this website, had sent advertising emails for other services, a new consent would be required for the new purpose. In addition, to comply with this requirement, the data controller must comply with the concept of purpose limitation under Article 5, Paragraph 1, Letter B, which states "*personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes*".

The criterion of specification in compliance with WP29 must be "*clearly and precisely to the scope and the consequences of the data processing*".[322]

Furthermore, as in the case of separate consent, in cases where the data processing is changed or added, the purpose of the consent is also changed, and the data controller must obtain new consent from the data subject.

It is important to be precise in saying that this requirement is closely linked with the requirement of informed consent.

---

[320] See, GDPR, Article 6, Paragraph 1, letter a.

[321] Ibid., Recital 43.

[322] See, WP 187, page 17.

c) The Criterion of Being Informed

The requirement of "informed" consent is based on the principle of transparency under Article 5, Paragraph 1, Letter A of the GDPR, which states "*personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*".

The data controller needs to provide information regarding knowledge of the parameters of the data processing to the data subject before obtaining her or his consent. The GDPR states that "*for consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended*".[323] In this regard, WP29 elaborated a list that defines "minimum content requirements for consent to be informed". According to this list, the minimum requirements are "*(i) the controller's identity, (ii) the purpose of each of the processing operations for which consent is sought, (iii) what (type of) data will be collected and used, (iv) the existence of the right to withdraw consent, (v) information about the use of the data for automated decision-making in accordance with Article 22 (2)(c) where relevant, and (vi) on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46*".[324]

The WP29 goes on to note that in some circumstances and contexts, "*more information may be needed to allow the data subject to genuinely understand the processing operations at hand*".[325] The data controller must make the data subject understand all elements of the data processing. The WP29 states, "*The more complex data processing is, the more can be expected from the data controller. The more difficult it becomes for an average citizen to oversee and understand all the elements of the data processing, the larger the efforts should become for the data*

[323] See, GDPR, Recital 42.

[324] See, WP259 rev.01, page 13.

[325] Ibid.

controller to demonstrate that consent was obtained based on specific, understandable information".[326]

In order to meet the requirement of informed consent, the GDPR does not prescribe in what form such information must be provided.[327] This complicates the understanding of when and how the consent of netizens is considered valid, which is already in the age of the Internet, this requirement is questionable as it cannot be guaranteed that all data subjects will be able to understand all elements of the data processing,[328] and by a research study conducted by a group of experts in this regard,[329] that not all websites do provide clear and complete information of the data processing to the data subject, they state "*on the basis of our analysis on the requirement for the consent to be informed, 184 websites (93.4 per cent) state the purposes of data processing in their respective privacy policies, although a significant portion of these websites fail to provide a clear and complete information on the conditions and purposes of such processing*".[330]

Even though this research was conducted in 2013, the problem still exists today, [331] as a recent study on cookie consent yielded a similar outcome.[332] Specifically, the authors underline that "*for the selected domains, we find that 94.7% contained*

---

[326] See, WP 187, page 21.

[327] See, EDPB, Guidelines 05/2020, Paragraph 66.

[328] J. Míšek, *Consent to personal data processing – The Panacea or The dead end?*, Masaryk University Journal of Law and Technology, 2014, page 74.

[329] M. Borghi, F. Ferretti, and S. Karapapa, *Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK*, International Journal of Law and Information Technology, Vol. 21, No. 2, 2013.

[330] See, Borghi, Ferretti, and Karapapa, page 139.

[331] D. Bollinger, K. Kubicek, C. Cotrini, D. Basin, *Automating Cookie Consent and GDPR Violation Detection*, Conference Paper, ETH Library, August 2022.

[332] Cookies are small text files that websites place on your device as you are browsing. Cookie consent is the website visitor's permission allowing a company to place a cookie in their browser to gather specific data about them. Cookie consent is required to lawfully obtain most of the different types of data you collect via your cookies.

at least one potential violation. In 36.4%, we found at least one cookie with an incorrectly assigned purpose, and in 85.8%, there was at least one cookie with a missing declaration or missing purpose. 69.7% of the sites assumed positive consent before it was given, and 21.3% created cookies despite negative consent".[333]
The GDPR makes it clear that in the absence of an adequacy decision or appropriate safeguards, the data controller can transfer personal data to a third country or international organisation with the consent of the data subject. The GDPR states that "*the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards*".[334]
Regarding the consent of the data subject in an online context, Advocate General Szpunar describes in the *Planet49* case that,[335] "*it must be made crystal-clear to a user whether the activity he pursues on the internet is contingent upon the giving of consent. A user must be in a position to assess to what extent he is prepared to give his data in order to pursue his activity on the internet. There must be no room for any ambiguity whatsoever. A user must know whether and, if so, to what extent his giving of consent has a bearing on the pursuit of his activity on the internet*".[336]

d) The Criterion of Non-Ambiguity

The last requirement of valid consent is that it must be unambiguous.[337]

---

[333] See Bollinger, Kubicek, Cotrini, Basin, page 2.

[334] See, GDPR, Article 49, Paragraph 1, letter a.

[335] See, Opinion of Advocate General Szpunar, of 21 March 2019, *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV*, Case C-673/17, ECLI:EU:C:2019:246.

[336] Ibi., Paragraph. 67.

[337] See, GDPR, Article 4, Paragraph 11.

The requirement of unambiguous means there is no doubt regarding the willingness of the data subject to express their consent. This requirement finds its discipline in recital 32 of the GDPR, which explains that "*consent should be given by a clear affirmative act establishing an…unambiguous indication of the data subject's agreement…such as by a written statement, including by electronic means, or an oral statement*".[338] According to the working paper on the GDPR,[339] a clear affirmative act could mean "*no doubt of the data subject's intention to consent, while making clear that – in the context of the on-line environment - the use of default options which the data subject is required to modify in order to reject the processing ("consent based on silence") does not in itself constitute unambiguous consent*".[340] In addition, in accordance with it, even though the DPD and its successor GDPR do not indicate a specific form for valid consent, consent based on silence, or so-called passive consent, is not acceptable. This orientation was then followed by Advocate General Szpunar, who in the *Planet49* case expresses the following opinion: "*I infer from this that it is not sufficient in this respect if the user's declaration of consent is pre-formulated and if the user must actively object when he does not agree with the processing of data*".[341] "*Indeed, in the latter situation, one does not know whether such a pre-formulated text has been read and digested. The situation is not unambiguous. A user may or may not have read the*

[338] Ibid., Recital 32.

[339] SEC(2012) 72 final, Commission Staff Working Paper, *Impact Assessment, Accompanying the document, Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, of 25 January 2012.

[340] Ibid., pages 105 and 106.

[341] See, Opinion of Advocate General Szpunar, Paragraph 60.

text. He may have omitted to do so out of pure negligence. In such a situation, it is not possible to establish whether consent has been freely given".[342]

The WP29 provides a clarification of the term "unambiguous", which means "*consent must leave no doubt as to the data subject's intention to deliver consent. In other words, the indication by which the data subject signifies his agreement must leave no room for ambiguity regarding his/her intent. If there is a reasonable doubt about the individual's intention, there is ambiguity*".[343]

2. The Prohibition of the Situation of "Bundling"

In the online environment, there is a very common situation where an online provider asks users in return to provide their personal data as an essential consideration; this situation is called "bundling" or "tying".

Bundling is prohibited by EU law. According to the EDPB, this situation represents a limitation of the consent of the data subject, particularly, the requirement of "freely given".[344] For the situation in question, it states that "*whenever a request for consent is tied to the performance of a contract by the controller, a data subject that does not wish to make his/her personal data available for processing by the controller runs the risk to be denied services they have requested*".[345] In addition, the EDPB specifies that, in the case of bundling, it is necessary to determine "*the scope of the contract…and what data would be necessary to performance of that contract*".[346] Consequentially, the EDPB makes clear that "*if a data controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis*".[347]

---

[342] Ibid., Paragraph 61.

[343] See, WP 187, page 21.

[344] See, EDPB, Guidelines 05/2020, page 10.

[345] Ibid., Paragraph 28.

[346] Ibid., Paragraph 29.

[347] Ibid., Paragraph 31.

The prohibition of bundling was confirmed by the CJEU in the *Planet49* case.[348] In this case, the subject of the dispute was an online promotional lottery organised by Planet49 GmbH.[349] To participate, users had to provide their name and address. They were presented with a webpage containing three items relevant to the legal review: two bodies of explanatory text, each accompanied by a checkbox, and a button that roughly read "*Click here to participate free of charge*". The first checkbox has not been pre-selected. The attached text essentially allowed third parties to contact users by post, telephone, email, etc. for advertising purposes. The second checkbox contained a pre-selected tick. The accompanying text read, "*I agree to the web analytics service Remintrex being used for me. This has the consequence that [Planet49] sets cookies, which enables Planet49 to evaluate my surfing and use behaviour on the websites of advertising partners and thus enables Remintrex advertising based on my interests....*". Therefore, the second pre-ticked checkbox allowed extensive cookie-based user tracking for advertising purposes. Before clicking the button to continue, users had to actively tick the first checkbox, while it was not mandatory to leave the second checkbox ticked. Users were free to untick the box and, in doing so, deny consent to the placement of cookies and subsequent tracking.

Three questions refer to the CJEU, all of which refer exclusively to the second pre-ticked checkbox.[350] Firstly, if consent is provided through a pre-selected checkbox that the user must deselect to deny consent, is it valid? Secondly, what information must the service provider provide as part of providing clear and complete information to the user, including the duration of the cookie operation and whether third parties have access to the cookies? Thirdly, when the information is

---

[348] See, Judgment of the Court, of Grand Chamber, of 1 October 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*, Case C-673/17, ECLI:EU:C:2019:801.

[349] Ibid., paras 25-31.

[350] Ibid., para 28.

stored or accessed, does this information constitute personal data under the data protection law?

Unsurprisingly, the CJEU ruled that a pre-ticked checkbox that the user must untick to opt out does not constitute valid consent to data processing. Thus, the consent of Planet 49 is not valid. Furthermore, for this case, Advocate General Szpunar affirms that "*for consent to be 'freely given' and 'informed', it must not only be active, but also separate. The activity a user pursues on the internet (reading a webpage, participating in a lottery, watching a video, etc.) and the giving of consent cannot form part of the same act. In particular, from the perspective of the user, the giving of consent cannot appear to be of an ancillary nature to the participation in the lottery. Both actions must, optically in particular, be presented on an equal footing. As a consequence, it appears to me doubtful that a bundle of expressions of intention, which would include the giving of consent, would be in conformity with the notion of consent under Directive 95/46*".[351]

Advocate General Szpunar continues to specify that "*the prohibition on bundling is not absolute in nature*",[352] so for the situation of "bundling", it is necessary to take into consideration the provision under Article 7, Paragraph 4 of the GDPR, which states "*when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract*".

To obtain the valid consent of the data subject, in addition to complying with the requirements set out above, it must also be taken into consideration in conjunction with other provisions of the GDPR. The main provisions that need to be considered are Article 7, which refers to conditions for consent; Article 8, which regards the condition of the child; and Article 9 concerns sensitive data processing.

---

[351] See, Opinion of Advocate General Szpunar, Paragraph 66.

[352] Ibid., Paragraph 98.

3. Conditions for the Consent of the Data Subject under the GDPR

Conditions for the valid consent of the data subject are contained under Article 7 of the GDPR. This article represents a novelty of the GDPR since there is not an exact equivalent article in the DPD.[353]

Article 7 of the GDPR is composed of four Paragraphs, which are established when the consent of the data subject is legitimate for data processing. The first Paragraph describes demonstrating consent; the second Paragraph analyses obtaining consent; the third Paragraph states the withdrawal of consent; and the last Paragraph focuses on the requirement of free consent. The latter point is already explained above. Thus, Article 7 complements the definition of the consent of the data subject.

a) Demonstrating the Consent of the Data Subject

Article 7, Paragraph 1, states "*where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data*". It means that data controllers need to prove that they have received valid consent to data processing from the data subject. This also implies that the burden of proof that the data subject has given valid consent to specific data processing lies with the data controller.

The burden of proof on the data controller is an implicit rule from the word "demonstrate" under Article 7, Paragraph 1. The situation was different compared to the proposal for the GDPR, which explicitly put the burden of proof on the head of the data controller.[354]

---

[353] E. Kosta, *Article 7. Conditions for consent. In: The EU General Data Protection Regulation (GDPR)*, edited by C. Kuner, L. A. Bygrave, and C. Docksey, Oxford University Press, 2020, pages 347-348.

[354] See, SEC(2012) 72 final, page 60.

b) Obtaining the Consent of the Data Subject

The GDPR does not regulate which form of consent the data subject must give. Article 7, Paragraph 2, addresses the case of a pre-formulated written declaration of consent, which affirms that "*if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding*".
Regarding this matter, the WP29 expressed that "*when consent is requested as part of a (paper) contract, the request for consent should be clearly distinguishable from the other matters. If the paper contract includes many aspects that are unrelated to the question of consent to the use of personal data, the issue of consent should be dealt with in a way that clearly stands out, or in a separate document. Likewise, if consent is requested by electronic means, the consent request has to be separate and distinct, it cannot simply be a paragraph within terms and conditions*".[355]

c) The Withdrawal of the Consent of the Data Subject

Compared to the GDPR and the DPD, the DPD does not have an explicit rule on the withdrawal of the consent of the data subject; under the DPD, the withdrawal of consent was recognised as a part of the data subject's right to information self-determination.[356] In the GDPR, the rule of the withdrawal of consent is contained under Article 7, Paragraph 3, which underlines that "*the data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent*

[355] See, WP259 rev.01, page 14.

[356] See, Kosta, Article 7. Conditions for consent, page 347.

shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent".

Legal scholars affirm that this article contains three norms and one qualification.[357] The first norm is that the data subject has the right to withdraw their consent at any time; the second one is that the data controller must inform the data subject, before getting their consent, that they have the right to withdraw consent. This notification requirement is complemented by other notification duties under Articles 13 of the GDPR, which concern information to be provided where personal data are collected from the data subject,[358] and 14 of the GDPR, which concern information to be provided where personal data have not been obtained from the data subject.[359] The third norm is that consent must be as easy to withdraw as it is to provide. Regarding the qualification concerns, this article makes clear that the withdrawal of consent does not affect the lawfulness of the data processing that was based on the consent before the withdrawal.

---

[357] Ibid., page 351.

[358] Article 13, Paragraph 2, letter c: In addition to the information referred to in Paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; Article 14, Paragraph 2, letter d: In addition to the information referred to in Paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

[359] 5. Article 13, Paragraph 4: Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information; Article 14, Paragraph 5, letter a: Paragraphs 1 to 4 shall not apply where and insofar as: (a) the data subject already has the information.

It should be noted that the withdrawal of consent does not apply in cases where the data processing does not require obtaining the consent of the data subject or in cases where the law provides for an exception.
In addition, it is necessary to differentiate between the withdrawal of consent and the right to object.
The withdrawal of consent concerns the processing of data that has previously obtained the consent of the data subject. Therefore, the data controller is not required to delete the personal data processed before the withdrawal of consent. On the other hand, the right to object affects all data processing for which the data subject has not given consent. Thus, the data controller must delete the personal data, except where there is no other legal ground for the processing.[360]

d) The Freely Given Consent of the Data Subject

"Freely given" consent means that the consent of the data subject must be given under a free decision, without any restriction by anyone. This is a fundamental element of obtaining valid consent.

Delving deeper into this context, it is crucial to emphasize that while the GDPR is founded on the principles of lawfulness, fairness, and transparency in the processing of personal data, [361] and establishes conditions for obtaining valid consent, [362] practical implementation often reveals that consent becomes more of a procedural formality than a conscious and informed act by the data subject.[363]

---

[360] See, GDPR, Article 17, Paragraph 1, letter b.

[361] See, GDPR, Articles 5, and 6.

[362] See, GDPR, Articles 7, and 8.

[363] W. Kotschy, *Article 6. Lawfulness of processing, in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020, pages 329-343.

4. *Conditions applicable to the Consent of Child about Information Society Services*

The consent of the child to data processing is a complicated legal issue, as it involves setting an age for the acquisition of certain rights or for the loss of certain protections. The GDPR introduced legal rules on the processing of data about children into the EU legal order for the first time, as the DPD does not regulate it.

Before the GDRP entered into force, the data processing of children followed guidelines published by WP29, which from 2009 had published several guidelines on the consent of children to the processing of their data.[364]

According to the Convention on the Rights of the Child of the United Nations, a child is someone under the age of 18, unless they acquire legal adulthood before that age.[365] The EU has adopted the same definition of a child as in this Convention.[366]

The GDPR underlines the importance of protecting children in data processing; it states that "*children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a*

---

[364] Article 29 Data Protection Working Party, *Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)*, WP 160, of 11 February 2009; Article 29 Data Protection Working Party, *Opinion 5/2009 on online social networking*, WP 163, of 12 June 2009; Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, WP 171, of 22 June 2010; and Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices*, WP 202, of 27 February 2013.

[365] United Nations, General Assembly resolution 44/25, *Convention on the Rights of the Child*, of 20 November 1989, Article 1.

[366] See, WP 160, page 3.

child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child".[367] This Recital does not specify whether it is necessary to regulate the processing of minors' data relating to online or offline services, but it is clear that it is important to protect the personal data of children both online and offline. Moreover, the GDPR specifies that the data controller should obtain the valid consent of the child by using an easily understood language.[368]

The GDPR has introduced the regulation of personal data protection for the protection of minors, in Article 8, which states "*in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years*". This implies that, in cases involving children under 16 or under the national age limit, consent must be authorized by the holder of parental responsibility. For the first time, the GDPR requires parental consent before information society service providers can process the personal data of children under 16 years of age.[369] Additionally, the data controller must verify that "*consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology*". It is also specified that the general contract law of EU Member States shall not be affected by the Paragraph 1 of Article 8.

It is evident from this definition that EU Member States have the flexibility to reduce the age of the child required to obtain valid consent from 16 years old to not

---

[367] See, GDPR, Recital 38.

[368] See, GDPR, Recital 58.

[369] M. Macenaite, and E. Kosta, *Consent for processing children's personal data in the EU: following in US footsteps?*, Information & Communications Technology Law, Volume 26, Issue 2, 2017, pages 1-2.

less than 13 years old. Allowing this flexibility may result in a lack of homogeneity among the legal systems of EU Member States. Therefore, legal scholars argue that EU legislators should dedicate more time and effort to balancing legal provisions on data protection for children.[370]

According to the EDPB Guidelines 05/2020, "*When providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities. When providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities. If the users state that they are over the age of digital consent then the controller can carry out appropriate checks to verify that this statement is true. Although the need to undertake reasonable efforts to verify age is not explicit in the GDPR it is implicitly required, for if a child gives consent while not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawful If the users state that they are over the age of digital consent then the controller can carry out appropriate checks to verify that this statement is true. Although the need to undertake reasonable efforts to verify age is not explicit in the GDPR it is implicitly required, for if a child gives consent while not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawfull. If the user states that he/she is below the age of digital consent then the controller can accept this statement without further checks, but will need to go on to obtain parental authorisation and verify that the person providing that consent is a holder of parental responsibility If the user states that he/she is below the age of digital consent then the controller can accept this statement without further checks, but*

[370] D. Krivokapić, and J. Adamović, *Impact of General Data Protection Regulation on Children's Rights in Digital Environment*, Belgrade Law Review, No. 3, 2016, pages 205-220.

will need to go on to obtain parental authorisation and verify that the person providing that consent is a holder of parental responsibility".[371] Additionally, the guidelines specify that "*Age verification should not lead to excessive data processing. The mechanism chosen to verify the age of a data subject should involve an assessment of the risk of the proposed processing*".[372]

As underscored by the EDPB, while the responsibility lies with the data controller to verify the age declared by users, practical implementation of these measures can be challenging.

Furthermore, Article 8 of the GDPR determines the conditions applicable to the consent of the child to information society services.

Since the definition affirms the consent of a child relating to information society services, at this point, it is necessary to define the meaning of information society services. Article 4, Paragraph 25, of the GDPR, refers to the definition of information society services in the Single Market Directive.[373] According to this Directive, information society services mean "*any information society service any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) 'at a distance means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of ser-*

[371] See, EDPB, Guidelines 05/2020, page 27, Paragraphs 132-134.

[372] Ibid, page 28, Paragraph 135.

[373] Directive 2015/1535 of the European Parliament and of the Council, of 9 September 2015, *laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification)*, O.J.E.U. L 241/1, of 17 September 2015.

vices' means that the service is provided through the transmission of data on individual request".[374]

The definition of information society services emphasises the requirement of "remuneration", and the definition of Article 8 of the GDPR states the requirement of "direct" services to children since it does not refer to all information society services but only those services offered directly to children.

a) The requirement of "remuneration"

The remuneration requirement does not mean only those situations of direct remuneration from the user; it is necessary to interpret it in a broad sense,[375] but also those cases when there is an "element of chance" inherent in the return.[376]

b) The requirement of "direct" services

Article 8 of the GDPR states consent "*in relation to the offer of information society services directly to a child*". The word "directly" does not refer only to services that are exclusively offered to children, as this requirement should be read broadly. Thus, information society services within the meaning of Article 8 mean those services that address children only or children and adults.[377]

---

[374] See, Directive 2015/1535, Article 1, Paragraph 1, letter b.

[375] R. Queck, A. de Streel, L. Hou, J. Jost, and E. Kosta, *The EU Regulatory Framework Applicable to Electronic Communications*, Telecommunications, Broadcasting and the Internet - EU Competition Law & Regulation, 2010, page 1-47.

[376] P. Craig, and G. de Búrca, *EU Law: Text, Cases, and Materials*, 4th Edition, Oxford University Press, 2008, page 819.

[377] E. Lievens, and V. Verdoodt, *Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation*, Computer Law & Security Review, Vol. 34, Issue 2, 2018, page 276.

5. Processing of Special Categories of Personal Data under the GDPR

Sensitive data is considered a special category of personal data. Therefore, the term "sensitive data" is used as a synonym for the special categories of personal data.[378]

Sensitive data, in general, are prohibited from being processed under Article 9 of the GDPR, so sensitive data are subject to more restrictive provisions than personal data considered non-sensitive in data processing.

Article 9 replaced Article 8 of the DPD. In addition, it contains some exceptions that allow the processing of sensitive data. The exceptions are the explicit consent of the data subject, the legal obligation of the data controller, vital interests, data processing by non-profit bodies, personal data manifestly made public by the data subject, legal claims, substantial public interest, public health, archiving in the public interest, scientific or historical research, or statistical purposes.

According to the opinion of the EU Commission, the processing of sensitive data must satisfy a legal basis under Article 6 of the GDPR and meet one of the situations covered in Article 9, Paragraph 2 of the GDPR.

a) Explicit consent of the data subject

Article 9, Paragraph 2, Letter A, states that the processing of sensitive data is permitted when the data subject gives explicit consent. The consent of the data subject represents a legal basis for data processing under Article 6 of the GDPR, but the latter does not mention having "explicit" consent, only standard consent.

Explicit consent means the consent of the data subject cannot be implied, and it is necessary to have definiteness in the declaration of consent. Explicit consent is also required for the transfer of personal data outside the EU under Article 49, Paragraph 1, Letter A, of the GDPR.

---

[378] See, GDPR, Recital 10.

b) Processing necessary to carry out the obligations and exercise specific rights of the controller or of the data subject in the field of employment and social security and social protection law

In labour matters, there is a power imbalance between employer and employee in data processing. Article 9, Paragraph 2, letter b, allows the employer, as the data controller, to process the sensitive data of the worker in case of the need to fulfil obligations and exercise specific rights of the controller or of the data subject in the field of employment, social security, and social protection law.

c) Protection of the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

This includes situations where data processing is necessary to protect the vital interests of the sensitive data subject since the data subject is physically or legally unable to consent. The GDPR states that "*the processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters*".[379] In addition, Recital 112 of the GDPR underlines that "*a transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential*

[379] See, GDPR, Recital 46.

for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent".

d) Processing is carried out during its legitimate activities with appropriate safeguards by a foundation, association, or any other not-for-profit body with a political, philosophical, religious or trade union aim

Article 9, Paragraph 2, Letter D, states "*processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects*".
Furthermore, the GDPR affirms that this exception applies only to those organisations whose purpose in processing sensitive data is to enable "the exercise of fundamental freedoms".[380] Thus, the exception covers only data processing carried out in connection with the purposes of the organisation and not every non-governmental or non-profit organisation.

e) Data is manifestly made public

Article 9, Paragraph 2, Letter E, of the GDPR pronounces "*personal data which are manifestly made public by the data subject*". It means that when the sensitive data processed is made public by the data subject, the data controller can process sensitive data. The word "manifestly" denotes publishing sensitive data as an affirmative act by the data subject, and the term "made public" represents sensitive

[380] Ibid., Recital 51.

data published in the mass media, online social network platforms, or similar actions.[381]

f) Legal claims and judicial activities

This exception, under Article 9, Paragraph 2, Letter F, of the GDPR, is to protect the right to an effective remedy and to a fair trial under Article 47 of the CFR and Article 6 of the European Convention on Human Rights.[382] It allows "*the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure*".[383]

g) Substantial public interest

According to Article 9, Paragraph 2, Letter G, of the GDPR "*processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law". In addition, the processing of sensitive data "shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*".

h) Healthcare and health provision

Article 9, Paragraph 2, Letter H, of the GDPR, contains a broad exception for the processing of sensitive data for healthcare purposes. This provision covers "*pre-*

[381] L. Georgieva, and C. Kuner, *Article 9. Processing of special categories of personal data. In: The EU General Data Protection Regulation (GDPR)*, edited by C. Kuner, L. A. Bygrave, and C. Docksey, Oxford University Press, 2020, page 378.

[382] Ibid., page 379.

[383] See, GDPR, Recital 52.

ventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional".

It should be noted that this provision does not apply to the processing of sensitive data for medical research purposes, as the latter is governed by Article 9, Paragraph 2, Letter I, of the GDPR.

Furthermore, pursuant to this exception, it is also necessary to satisfy the requirements of Article 9, Paragraph 3, of the GDPR, which requests that the sensitive data be "*processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies*".

i) Public interest in public health

Article 9, Paragraph 2, Letter I of the GDPR, allows the processing of sensitive data when "*processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy*". The term "public interest" is defined as "*all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and uni-*

versal access to, health care as well as health care expenditure and financing, and the causes of mortality".[384]

Under this exception, the right to erasure does not apply.[385]

Archiving purposes in the public interest, scientific or historical research purposes or statistical purpose

This provision underlines that the processing of sensitive data is possible when it is necessary "*for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*".[386]

[384] Ibid., Recital 54.

[385] Ibid., Article 17, Paragraph 3, letter c.

[386] Ibid., Article 9, Paragraph 2, letter j.

Chapter 3
The Consent of Information Subject to Information Processing in Chinese Legal Instruments

1. The Consent of the Information Subject under the Chinese Civil Code and the PIPL

The provisions of the consent of the information subject in the Chinese legal system are primarily contained under the Chinese Civil Code and the Chinese Personal Information Protection Law (PIPL). It can also find some general notions under the Chinese Cybersecurity Law (CSL), which before the enactment of the PIPL, had been the main law to protect personal information in China. The CSL is still in effect, but the rules on personal information protection are now also contained in the PIPL in a more detailed and less restrictive way.[387] Therefore, this Chapter deals only with the provisions contained in the civil code and in the PIPL to avoid repetitions.

Article 1035, Paragraph 1 of the Chinese Civil Code states "*The processing of personal information shall be in compliance with the principles of lawfulness, justification, and within a necessary limit, and shall not be excessively processed; meanwhile, the following conditions shall be satisfied consent has been obtained from the natural person or his guardian, unless otherwise provided by laws or administrative regulations*".[388] In addition, Article 13 of the PIPL affirms, "*A personal information processor can process personal information of an individual only if one of the following circumstances exists: (1) the individual's consent has been obtained; (2) the processing is necessary for the conclusion or performance*

[387] See, Part 1, Chapter 3, Paragraph 2.

[388] Translated by the National People's Congress (NPC), the original text is "处理个人信息的, 应当遵循合法, 正当, 必要原则, 不得过度处理, 并符合下列条件征得该自然人或者其监护人同意, 但是法律, 行政法规另有规定的除外".

of a contract in which the individual is a party, or necessary for human resources management in accordance with the labor rules and regulations established in accordance with the law and the collective contracts signed in accordance with the law; (3) the processing is necessary for the performance of statutory duties or obligations; (4) the processing is necessary for the response to public health emergencies, or for the protection of life, health, and property safety of natural persons in emergencies; (5) the personal information is reasonably processed for news reporting, media supervision, and other activities conducted in the public interest; (6) the personal information disclosed by the individual himself or other legally disclosed personal information of the individual is reasonably processed in accordance with this Law; and (7) other circumstances as provided by laws or administrative regulations".[389] Furthermore, Article 13, Paragraph 2 of the PIPL underlines that "*Individual consent shall be obtained for processing personal information if any other relevant provisions of this Law so provide, except under the circumstances specified in Subparagraphs (2) to (7) of the preceding paragraph*".[390] These situations in Paragraphs (ii) to (vii) constitute the cases of exception for personal information processing. Regarding the cases of obtaining consent, the information disclosed by the natural person himself or the other information that has already been legally disclosed, and to protect the public interest or

[389] Translated by the National People's Congress (NPC), the original text is "符合下列情形之一的，个人信息处理者方可处理个人信息：（一）取得个人的同意；（二）为订立, 履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；（三）为履行法定职责或者法定义务所必需；（四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；（五）为公共利益实施新闻报道, 舆论监督等行为，在合理的范围内处理个人信息；（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；（七）法律, 行政法规规定的其他情形".

[390] Translated by the National People's Congress (NPC), the original text is "依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意".

the lawful rights and interests of the person, under Article 1036 of the Chinese Civil Code, the information subject "*shall not bear civil liability*".

Under these two rules, "consent" represents one of the legal bases for lawful personal information processing. Article 14, Paragraph 1 of the PIPL describes the requirements for obtaining valid consent, which outlines that "*Where personal information processing is based on individual consent, the individual consent shall be voluntary, explicit, and fully informed*".[391] According to this article, to obtain valid consent, one needs to satisfy the two requirements, which are "the precondition of full knowledge" and "voluntary and explicit manner".

The requirement of "the precondition of full knowledge" represents that the information controller shall inform the information subject of all details of the processing before starting the information process. It is a precondition of personal information processing, and the requirement of a "voluntary and explicit manner" means the consent is free and unambitious.

In addition, Article 14, Paragraph 1, continues to underline that the discipline contained in Paragraph 1 will apply only "*Where any other law or administrative regulation provides that an individual's separate consent or written consent must be obtained for processing personal information, such provisions shall apply*".[392] Thus, the PIPL has introduced a new regulation of the consent of the information subject to the processing of personal information and has divided the consent for the processing of information into two types: the general one (一般同意，

[391] Translated by the National People's Congress (NPC), the original text is "基于个人同意处理个人信息的, 该同意应当由个人在充分知情的前提下自愿,明确作出.. 个人信息的处理目的, 处理方式和处理的个人信息种类发生变更的, 应当重新取得个人同意".

[392] Translated by the National People's Congress (NPC), the original text is "法律, 行政法规规定处理个人信息应当取得个人单独同意或者书面同意的, 从其规定".

yībāntóngyì) and the special one (单独同意，dāndútóngyì).[393] There is no definition of general consent in the Chinese civil code or PIPL, and they do not provide any details on the requirement or form of general consent. This point will be elaborated upon later.

Additionally, Article 14, Paragraph 2, clarifies that in the event "*In the case of any change of the purposes or means of personal information processing, or the category of processed personal information, a new consent shall be obtained from the individual*". [394] This is the situation called reobtain consent (重新同意, Chóngxīntóngyì).

Furthermore, the PIPL, under Article 16, states that "free consent" means that "*A personal information processor shall not refuse to provide products or services for an individual on the grounds that the individual withholds his consent for the processing of his personal information or has withdrawn his consent for the processing of personal information, except where the processing of personal information is necessary for the provision of products or services*".[395] It indicates that the information controller, before obtaining the consent of the information subject, needs to inform the personal information subject of every detail about the personal information process, and the information subject needs to feel free and without any restrictions or misunderstandings when giving their consent to the processing of personal information. Article 16 also affirms that it prohibits bundling.

---

[393] To be specific, the PIPL provides multiple types of consent: general consent, separate consent, reobtain consent (Article 14, Paragraph 2 of the PIPL), and legal guardian consent (Article 31 of the PIPL).

[394] Translated by the National People's Congress (NPC), the original text is "个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意".

[395] Translated by the National People's Congress (NPC), the original text is "个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由, 拒绝提供产品或者服务; 处理个人信息属于提供产品或者服务所必需的除外".

2. *Separate Consent and Written Consent under the PIPL*

Separate consent is also known as "individual consent", "unilateral consent" or "specific consent".[396] Separate consent differs from general consent, as in addition to having to satisfy the requirements of Article 16 of the PIPL, separate consent is provided only for the cases strictly foreseen by the law, which are when the personal information processor transfers personal information to other controllers,[397] to disclose publicly processed personal information,[398] facial recognition collected in public venues for other purposes, excluding the purpose of ensuring public security,[399] processing sensitive personal information,[400] and cross-border transfer of personal information.[401] Furthermore, separate consent is considered a higher level of personal information processing requirement.[402]

Concerning sensitive personal information, in addition to having separate consent to process it, it is also necessary to specify the purpose,[403] to further the protection of the personal information of the information subject.[404]

---

[396] F. Guo, L. Chen, and Y. Jia, *《个人信息保护法》具体适用中的若干问题探讨 - 基于《民法典》与《个人信息保护法》关联的视角* (《Gèrén xìnxī bǎohù fǎ》 jùtǐ shìyòng zhōng de ruògān wèntí tàntǎo —jīyú 《mínfǎ diǎn》 yǔ 《gèrén xìnxī bǎohù fǎ》 guānlián de shìjiǎo), 法律适用 (Fǎlǜ shìyòng), No. 1, 2022, page 16.

[397] See, PIPL, Article 23.

[398] Ibid., Article 25.

[399] Ibid., Article 26.

[400] Ibid., Article 29.

[401] Ibid., Article 39.

[402] X. Xiao, *Pluralistic Rules on Consent for Personal Information Processing-Analysis and Interpretation based on the Stratum System of Consent (个人信息处理的多元同意规则-基于同意阶层体系的理解和阐释)*, 政治与法律 (Zhèngzhì yǔ fǎlǜ, Politics and Law), No. 4, 2022.

[403] See, PIPL, Article 28, Paragraph 2.

[404] L. Wang, *Mǐngǎn gèrén xìnxī bǎohù de jīběn wèntí -yǐ «mínfǎ diǎn» hé «gèrén xìnxī bǎohù fǎ» de jiěshì wèi bèijǐng (敏感个人信息保护的基本问题-以《民法典》和《个人信息保护法》的解释为背景, Basic Issues of Sensitive Personal Information Protection-With the background of in-*

Separate consent can be replaced by written consent. Article 469, Paragraph 2, of the Chinese Civil Code, contained under Chapter II on Conclusion of Contracts, provided a definition of written consent, which is "*A writing refers to any form that renders the content contained therein capable of being represented in a tangible form, such as a written agreement, letter, telegram, telex, or facsimile*".[405]

3. The Consent of Children under the PIPL

The purpose of legally establishing an age standard for "the consent of children" as an information subject is to provide an objective measure for judging whether the "consent" given by a child is valid or not. Article 31 of the PIPL establishes the autonomy of giving consent to the processing of personal information from the age of 14. It is earlier than the age of majority, which is foreseen at the age of 18.[406] In the case of children under the age of 14, the processing of personal data must be authorised by the person exercising parental permission over the minor to avoid violating the regulations of children's guardians in China.[407] This type of consent is called legal guardian consent (监护人同意, Jiānhùréntóngyì).

Article 31, Paragraph 1 of the PIPL states that "*To process the personal information of minors under the age of 14, personal information processors shall obtain the consent of the parents or other guardians of the minors*".[408] In addition,

---

terpretation of «Civil Code» and «Personal Information Protection Law»), Dāngdài fǎxué (当代法学, Contemporary Jurisprudence), No. 1, 2022.

[405] Translated by the National People's Congress (NPC), the original text is "以电子数据交换, 电子邮件等方式能够有形地表现所载内容,并可以随时调取查用的数据电文, 视为书面形式".

[406] See, Chinese Civil Code, Article 17.

[407] K. Feng, *Age Criteria of "Children's Consent" in Personal Information Processing (个人信息处理中"儿童同意"的年龄标准)*, Jinan Journal, Philosophy & Social Sciences, No. 8, 2021.

[408] Translated by the National People's Congress (NPC), the original text is "个人信息处理者处理不满十四周岁未成年人个 人信息的, 应当取得未成年人的父母或者其他监护人的同意".

Paragraph 2 continues to describe that "*Personal information processors processing the personal information of minors under the age of 14 shall develop special rules for processing such personal information*".[409]

4. *The Withdrawal of the Consent of the Information Subject under the PIPL*

The PIPL expects the right to withdraw the consent of the information subject under Article 15.

Article 15, Paragraph 1, states that "*Where personal information processing is based on individual consent, an individual shall have the right to withdraw his consent*".[410] In addition, "*Personal information processors shall provide convenient ways for individuals to withdraw their consents*".[411] Furthermore, Paragraph 2 clarifies that "*The withdrawal of consent shall not affect the validity of the processing activities conducted based on consent before it is withdrawn*".[412]

It should be noted that personal information processors cannot refuse to provide products or services if the information subject withdraws their consent.[413] Additionally, under Article 47 of the PIPL, the personal information processor shall proactively delete personal information where the information subject withdraws their consent, and "*a personal information processor shall take the initiative to*

---

[409] Translated by the National People's Congress (NPC), the original text is "个人信息处理者处理不满十四周岁未成年人个人信息的,应当制定专门的个人信息处理规则".

[410] Translated by the National People's Congress (NPC), the original text is "基于个人同意处理个人信息的，个人有权撤回其同意".

[411] Translated by the National People's Congress (NPC), the original text is "个人信息处理者应当提供便捷的撤回同意的方式".

[412] Translated by the National People's Congress (NPC), the original text is "个人撤回同意,不影响撤回前基于个人同意已进行的个人信息处理活动的效力".

[413] See, PIPL, Article 16.

erase personal information, and an individual has the right to request the deletion of his personal information".[414]

The right to withdrawal does not apply to personal information processing activities based on a legal basis other than consent.

[414] Translated by the National People's Congress (NPC), the original text is"个人信息处理者未删除的，个人有权请求删除".

Conclusion of Part 3

The consent of the data (information) subject to personal data (information) processing represents the legal basis for lawful processing under international, EU, and Chinese legal instruments.

The concepts of consent under international, EU, and Chinese legal instruments are quite similar but not the same, with some noticeable differences between them.

The provisions of consent under international legal instruments are almost identical to the provisions of consent contained in EU legal instruments, particularly the provisions contained in the GDPR. With only two differences, the first, under international legal instruments on data protection, does not provide a definition of the consent of the data subject.[415] Another difference is that the provisions envisaged in international legal instruments must be viewed from the point of view of the right to privacy and not that of the right to data protection. Indeed, the ECtHR declares that in the case of disclosure of personal information without the consent of the data subject, there is a violation of the right to respect for private and family life, home, and correspondence under Article 8 of the European Convention on Human Rights.[416] This perspective described in the international legal instruments complies with the international legal framework on data protection since, as explained in Part 1, Chapter 1, Paragraph 2, the international legal order does not recognise the right to data protection as an individual and distinct right.

On the other hand, the differences are more significant between the EU legal instruments and the Chinese legal instruments on this matter.

---

[415] L. A. Bygrave, and L. Tosoni, *Article 4(11). Consent In: The EU General Data Protection Regulation (GDPR)*, edited by C. Kuner, L. A. Bygrave, and C. Docksey, Oxford University Press, 2020, page 178.

[416] Council of Europe, European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights-Right to respect for privacy and family life, home and correspondence*, 31 August 2022, pages 38-46.

Firstly, under the GDPR, there is only one figure for the data subject's consent. Instead, in the Chinese legal system, there are generally two kinds of consent from the information subject: “general consent” and “separate consent”. The PIPL affirms that separate consent is requested only for cases dictated by law, and it explains only the requirements of the separate consent of the information subject and does not give details about the general consent. The GDPR states it is necessary to satisfy four criteria to obtain valid consent, which are free consent, specification, being informed, and unambiguous, and the PIPL requests only two requirements, which are the requirement of “the precondition of full knowledge”, and the requirement of a “voluntary and explicit manner”. Even though the number of requirements between the EU and Chinese legal instruments is different, the required content is the same. It can be said that the requirement of “the precondition of full knowledge” under the PIPL includes the criteria of specification and the criteria of being informed under the GDPR, and the requirement of a “voluntary and explicit manner” under the PIPL can imply the criteria of free consent and the criteria of an unambiguous request under the GDPR. In this sense, compared with the GDPR, separate consent in the PIPL is more like the concept of consent under the GDPR. Also, the GDPR mentions the term “separate consent”, but separate consent in the GDPR means new consent where the data processing is changed or added. Thus, it has a different concept with separate consent under the PIPL. The separate consent of the PIPL is more like a special consent for certain data processing.

Secondly, in China, there are conflicts of opinion among scholars regarding the concept of consent contained in the PIPL, as the PIPL dictates the two above requirements of valid consent but does not specify how and in what form these requirements need to be met; therefore, some scholars state that consent stated in the PIPL is an 知情同意 (zhīqíngtóngyì), while others state it is a 告知同意

(gàozhītóngyì).[417] 知情同意 and 告知同意 can both translate into English with the term "informed consent", but if it needs to differentiate them, it can translate the term "知情同意" with "informed consent" and the term "告知同意" with "to be informed". The core of the "知情同意" (informed consent) rule is to respect the will of the information subject; it places more emphasis on whether the information subject knows the purpose and method of the information handler's processing behaviour, etc. Instead, the term "告知同意" (to be informed) emphasises informed behaviour.

In my opinion, the PIPL contains both notions, precisely as it contains two kinds of consent. "知情同意" (informed consent) is required for separate consent due to the requirement of a "voluntary and explicit manner", so the information subject must know every detail about the information processing, and "告知同意" (to be informed) is for general consent since it seems that the act of informing is more important than the informed content.

Third, both the EU and Chinese legal instruments have provided for the regulation of the consent of children, but between them, there is a seeming difference in the age of the child; in the GDPR, parental permission is required for data processing before the age of 16. Instead, in the PIPL, it is necessary for parental permission to obtain consent to information processing when the child is under 14. In addition, the PIPL explicitly requires that specific rules be followed for the processing of personal data about children.

While all three legal frameworks uphold the principles of lawfulness, fairness, and transparency in the processing of personal data and establish conditions for obtaining valid consent, practical scenarios often reveal that, in the execution of these rules, consent becomes more of a procedural formality without the necessary awareness of the data subject.

---

[417] B. Lu, *个人信息保护的"同意"困境及其出路 (Gèrén xìnxī bǎohù de "tóngyì" kùnjìng jí qí chūlù, The "consent" dilemma of personal information protection and its way out)*, Studies in Law and Business, Vol. 38, No. 2, 2021.

This phenomenon may stem from various factors, including the complexity of privacy notices, a lack of clarity in legal language, or even the presence of pre-selected options in online consent forms. In many instances, data controllers may seem more focused on quickly obtaining consent rather than ensuring that data subjects fully comprehend the implications of the processing of their personal data.

Moreover, the context in which consent is collected must be taken into account. For instance, in digital environments such as websites or apps, the need to obtain consent can often clash with users' haste in navigating and accessing content. This can lead to a sort of automatic acceptance without a genuine evaluation of the provided information.

Similar challenges arise when considering the responsibility of data controllers to verify the age declared by users; however, in practice, these verification measures can be difficult to implement.

PART 4
THE RIGHTS OF NETIZENS AS DATA SUBJECT

The right to personal data protection is a fundamental right recognised by various legal systems. Legal instruments pertaining to personal data protection delineate this right into various sub-rights. Different legal instruments reserve different sub-rights, which are generally known as "the rights of data subjects". Consequently, netizens, as data subjects, are entitled to enjoy these sub-rights.

In essence, to uphold the rights of data subjects, the processing of personal data must adhere to the principles of lawfulness, fairness, and transparency; purpose limitation; data minimisation; data accuracy; storage limitation; and integrity and confidentiality.

The rights of data subjects constitute the core of personal data legal instruments, making them a fundamental focus of this research. Therefore, this part will describe the rights of data subjects under international, EU, and Chinese legal systems.

In this part, the international legal framework will primarily analyse Convention 108, as it is the only legal instrument with a binding authority in this context. Other international legal instruments do not offer specific rules or recommendations regarding data subjects' rights. Among the international legal instruments examined, the OECD Privacy Framework 2013 stands as an exception, recommending that data subjects should have the right to access, erase, rectify, or amend personal data in case of "personal data is challenged".

This part will be divided into three Chapters: the first Chapter will delve into the rights of data subjects under Convention 108; the second will expound on data subjects' rights under GDPR; and the final Chapter will elucidate the rights of information subjects within the Chinese legal system, with a particular focus on the Chinese Civil Code and the PIPL. The part will conclude with a comparative

analysis of the rights of data subjects among these aforementioned legal instruments.

Chapter 1
The Rights of Data Subjects under Convention 108

Convention 108 is the only binding international legal instrument regarding personal data protection. Under the Modernised Convention 108, the rights of data subjects are divided into five sub-rights, which are the rights to be informed, of access by the data subject, to restriction or erasure, to object, and related to automated decision-making.

1. The Right to Be Informed

Article 8 of the Modernised Convention 108 regulates the principle of transparency in personal data processing, which can translate into the right to be informed of data subjects, also known as the right to information, which states "*Each Party shall provide that the controller informs the data subjects of his or her identity and habitual residence or establishment; the legal basis and the purposes of the intended processing; the categories of personal data processed; the recipients or categories of recipients of the personal data, if any; and the means of exercising the rights set out in Article 9, as well as any necessary additional information in order to ensure fair and transparent processing of the personal data*". It means that at the time personal data is collected, the data controller or processor must inform the data subject regarding the personal data processing. It is also significant this is an obligation imposed on data controllers or processors that they need to comply with, regardless of the interest of the data subject.[418]

The modality of exercise of the right to be informed is also underlined in Article 9 Paragraph 1 Letter B of Convention 108, which says "*to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the*

[418] See, Council of Europe, Handbook on European data protection law, pages 212-215.

processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8, paragraph 1".

The information must be transparent, intelligible, easily understandable language, and easily accessible.[419]

2. *The Right of Access by the Data Subject*

The right of access is governed under Article 9 letter B of the Modernised Convention 108, which provides "*to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8, paragraph 1*". This provision was already foreseen in the original version of Convention 108 under Article 8 letter B and seeks to ensure the principle of transparency.

The right to access means the data subject needs to be informed regarding the origin of the personal data, the retention period, and all other information the data controller or processor must notice to the data subject.

Convention 108 does not make clear to the data subject from whom they should obtain confirmation that personal data are being processed or from whom the personal data are to be communicated. The Explanatory Report to the Modernised Convention seeks to make it clear that "*in most cases, this will be the controller or*

[419] Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights, Handbook on European data protection law: 2018 edition, Publications Office, 2019, pages 212-215.

the processor on his or her behalf. In exceptional cases, the means to exercise the rights to access, rectification, and erasure may involve the intermediary of the supervisory authority".[420]

Due to the particularity of the right to personal data protection in the international legal system,[421] the ECtHR points out that the right of access emerges to protect the right to respect private life.[422]

3. The Right to Rectification or Erasure

The right to rectification was one of the first rights granted to data subjects in international legal instruments on personal data protection.[423]

The right to rectification is regulated under Article 9 letter E of the Modernised Convention 108, which states "*to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention*". This provision was contained under Article 8 letter C in the original Convention 108 version, but it was expressed as a safeguard and not as a right.

The right to rectification is relevant when there is an error in personal data; indeed, according to the Explanatory Report of Convention 108, the right to rectification applies when there is "*erroneous or inappropriate information*" on personal data.[424]

---

[420] See, Explanatory Report to the Modernised Convention, point 74, page 13.

[421] See, Part 1, Chapter 1.

[422] See, Judgment of the ECtHR, *Godelli v. Italy*, no. 33783/08, of 25 September 2012.

[423] C. De Terwangne, *Article 16. Right to rectification, in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020, page 472.

[424] Council of Europe, European Treaty Series - No. 108, *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, page 10.

In terms of the application of this right, the ECtHR stated that when the request for rectification is based on unsubstantiated grounds and purely subjective, controllers can require objective evidence. Instead, when the error is detectable, the request of controllers to prove the evidence is considered, according to the ECtHR, a violation of the right to respect for private and family life, home, and correspondence under Article 8 of the ECHR.[425] To be precise, in some situations, the request for rectification is sufficient in a very simple way, such as in the situation of correcting the spelling of a name, a change of address, or a telephone number.[426]

The right to rectification can only be exercised for its own personal data, and controllers must rectify without undue or excessive delay.

The ECtHR also stated that public authorities could also commit a violation of Article 8 of the ECHR,[427] which means that data subjects can also exercise the right to rectification or erasure to public bodies.

4. The Right to Object

The right to object is a novelty of the Modernised Convention 108 compared to the original version.

Before the Modernised Convention 108, even though there was no right to object, the ECtHR had applied in many cases, and it said that the right to object was not considered a general right; it could be exercised in some situations.[428]

---

[425] See, Judgment of the ECtHR, *Ciubotaru v. Moldova*, no. 27138/04, of 27 April 2010.

[426] See, Council of Europe, Handbook on European data protection law: 2018 edition, pages 219-221.

[427] See, Judgment of the ECtHR, *Cemalettin Canli v. Turkey*, no. 22427/04, of 18 November 2008.

[428] See Judgment of the ECtHR, *Leander v. Sweden*, no. 9248/81, of 26 March 1987, Judgment of the ECtHR, *M.S. v. Sweden*, no. 20837/92, of 27 August 1997, and Judgment of the ECtHR, *Mosley v. the United Kingdom*, no. 48009/08, of 10 May 2011.

The right to object means data subjects have the right to stop or prevent the data controller from using their personal data. According to Article 9 letter D of the Modernised Convention 108, data subjects can "*object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms*". This also means that the burden of proof lies with the data controller.

5. The Right related to Automated Decision-Making

The right related to automated decision-making is a right that applies in the context of artificial intelligence (AI). If personal data is processed entirely by automatic means and this might have a legal or similarly significant effect on the person, data subjects can request some human involvement. Article 9, Paragraph 1 of the Modernised Convention 108 stipulates, "*(a) every individual shall have a right not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;… (c) to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her*".
Article 9, Paragraph 2, derogates the right related to automated decision-making "*if the decision is authorised by a law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests*".

Chapter 2
The Rights of Data Subjects under the GDPR

The GDPR represents the primary legal instrument in EU law regarding data subject protection. According to the GDPR, there are eight sub-rights to the rights of data subjects. Compared with the DPD, the GDPR reinforced rights and introduced some new rights.

The eight sub-rights are the right to be informed, the right of access by the data subject, the right to rectification, the right to erasure (right to be forgotten), the right to restriction of processing, the right to data portability, the right to object, and the right related to automated individual decision-making, including profiling.

1. The Right to Be Informed

The right to be informed means that the data controller or processor lets data subjects know how their personal data will be used, how long it will be kept, and whether their personal data will be shared with third parties or not.[429]

The right to be informed stems from transparency, fairness, privacy, and autonomy fundamental principles of the GDPR.[430]

To comply with this right, the GDPR divides into two different situations: the first, personal data collected from the data subject, and the second, personal data not collected from the data subject.

The first situation is governed under According to Article 13, Paragraph 1 of the GDPR, which states "*Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller and, where applicable, of the control-*

[429] See, GDPR, Recital 39.

[430] H. U. Vrabec, *Data Subject Rights under the GDPR*, Oxford Press, 2021.

ler's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available". To grant the principle of fair and transparent processing, Paragraph 2 continues to say, "*In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (d) the right to lodge a complaint with a supervisory authority; (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*". In addition, Paragraph 3 underlines "*Where the con-*

troller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2". This provision does not apply "*where and insofar as the data subject already has the information*".[431]

The second situation is contained under Article 14, Paragraph 1 of the GDPR, which stipulates "*Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) the categories of personal data concerned; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available*". Paragraph 2, to ensure fair and transparent processing, the controller shall provide the data subject with the following information: "*(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability; (d) where processing is based on*

[431] See, GDPR, Article 13, Paragraph 4.

point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (e) the right to lodge a complaint with a supervisory authority; (f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources; (g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject". In addition, the provision specifies, under Paragraph 3, that the controller shall provide the information "*(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed*". Paragraph 4 affirms "*Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information*", and Paragraph 5 lists the cases in which paragraphs 1-4 are inapplicable, which are "*(a) the data subject already has the information; (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available; (c) obtaining or disclosure is expressly laid down by Union or Member State law to*

which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy".

In short, controllers shall provide a detailed list of the information to the data subject at the time of collecting or obtaining the personal data, including the information regarding the right to lodge a complaint in cases of personal data breaches. The information must be in writing or other forms, including electronic forms,[432] within the respective time limits.

Before the GDPR came into force, the scope of the right to be informed and its limitations under EU law were explained in the cases of the Court of Justice of the European Union (CJEU). Two relevant cases are *Institut Professionnel des agents immobiliers (IPI) v. Englebert*,[433] and *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others*.[434] In the case *Institut Professionnel des agents immobiliers (IPI) v. Englebert*, the CJEU clarified that EU Member States may provide in their national legal system the exceptions for the obligation to inform data subjects; in the absence of any provision of exception, the data subject must be informed. And in the case of *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others*, the CJEU stated that when transferring personal data between public administrative bodies, the data subject should have been informed before the transfer, excluding only cases of safeguarding an important economic interest of the state and taxation matters, but restrictions must be imposed by legislative measures. In all other cases, the public administrative bodies must inform the data subject.

---

[432] See, GDPR, Articles 13, Paragraph 2, letter d, and 14, Paragraph 2, letter e.

[433] See, Judgment of the CJEU, of 7 November 2013, *Institut Professionnel des agents immobiliers (IPI) v. Englebert*, case C-473/12, ECLI:EU:C:2013:715.

[434] See, Judgment of the CJEU, of 1 October 2015, *Națională de Asigurări de Sănătate and Others*, case C-201/14, ECLI:EU:C:2015:638.

2. The Right of Access by the Data Subject

Alongside the right to be informed, under which controllers shall provide information to the data subject before data processing begins, there is the right of access to the data subject, which applies after data processing starts. The right of access is governed under Article 15 of the GDPR, which states, "*1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. 2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer. 3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information*

shall be provided in a commonly used electronic form. 4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others".

The right of access ensures a fundamental right of the data subject and the principles of fairness and transparency in data processing.[435] This affirmation is also confirmed by the CJEU's case.[436] Moreover, the CJEU declares the right of access must necessarily relate to the past; otherwise, the data subject would not be able to effectively exercise their right, that is, to rectify or block or bring legal processing and obtain compensation for the damage suffered.[437]

The right of access is also considered similar by the CJEU to the right of access to governmental rights, also known as the freedom of information, which ensures the transparency of the decision-making process of the public authorities.[438]

The right of access allows individuals to check whether their personal data is processed or not.[439] This is an important legal option for netizens to understand their data location and flows. For instance, if some people are not Facebook members and they surf Facebook's public pages, their personal data, such as their IP address, may be used for advertisement purposes.[440] Consequently, the right of ac-

---

[435] See, GDPR, Recital 63.

[436] See Judgment of the CJEU, of 17 July 2014, *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S,* joined cases C-141/12, and C-373/12, ECLI:EU:C:2014:2081., and Judgment of the CJEU, of 16 July 2015, *ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority*, case C-615/13, ECLI:EU:C:2015:489.

[437] See, Judgment of the CJEU, of 7 May 2009, College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer., case C-553/07, ECLI:EU:C:2009:293.

[438] See, Judgment of the CJEU, of 29 June 2010, *European Commission v The Bavarian Lager Co. Ltd.*, case C-28/08, ECLI:EU:C:2010:378.

[439] See, Vrabec, pages 104-108.

[440] See, Judgment of the CJEU, of Grand Chamber, of 15 June 2021, *Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit (Belgian Privacy Commission)*, case C-645/19, ECLI:EU:C:2021:483.

cess should permit non-registered users to know whether their personal data is processed or not and in what way.[441]

3. The Right to Rectification

The right to rectification grants data subjects the ability to request corrections to their personal data in the event of inaccuracies. This provision aligns with the principle of accuracy, which is crucial for maintaining a high standard of data protection for the data subject.[442]

The regulatory framework for the right to rectification is established in Article 16 of the GDPR, which stipulates, "*The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement*". According to this definition of the right to rectification, data subjects also have the right to complete their personal data in case it is incomplete. This incompleteness must be assessed in relation to the purposes of the processing.[443]

4. The Right to Erasure (the Right to Be Forgotten)

The right to erasure, also known as the right to be forgotten, allows data subjects to request the deletion or forgetting of their personal data by data controllers. This right aligns with the principle of data minimization,[444] which stipulates that per-

---

[441] See, Vrabec, pages 104-108..

[442] See, GDPR, Article 5, Paragraph 1, letter D.

[443] De Terwangne, Article 16. Right to rectification, page 473.

[444] See, GDPR, Recital 156.

sonal data should only be processed for specific and limited purposes.[445] Additionally, the right to erasure, does not apply to scientific, historical, or statistical research, regardless of public interest.

Although the right to erasure was mentioned in Article 12 of the DPD, it represents a significant innovation in the GDPR.[446] The GDPR not only includes the concept of "erasure" but also incorporates the idea of being "forgotten".[447]

The right to erasure is regulated by Article 17 of the GDPR. According to Article 17, Paragraph 1 of the GDPR, the data subject are granted the right to erasure when the following conditions are met: " *(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)*". Article 17, Paragraph 2, and Recital 66 of the GDPR underscore the need to consider available technologies and associated costs when implementing the right to erasure. In addition, Article 17, Paragraph 3, specifies situations in which the right to erasure should not be applied: "*(a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation*

---

[445] See, GDPR, Article 5.

[446] P. Voigt, and A. Von Dem Bussche, *The EU General Data Protection Regulation (GDPR) A Pratical Guide*, Springer International Publishing, 2017.

[447] H. Kranenborg, *Article 17. Right to erasure ("right to be forgotten"), in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020, page 477.

which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims".

The right to erasure has garnered significant attention from the public and legislators, particularly in the context of the *Google Spain* case.[448] In the *Google Spain* case, the CJEU was tasked with establishing the limits of the scope of application of the right to erasure. The Court interpreted the DPD, which was in force at the time, and declared that "*the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's*

[448] See, Judgment of the CJEU, of Grand Chamber, of 13 May 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, case C-131/12, ECLI:EU:C:2014:317. (*The Google Spain case, officially known as "Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González," is a landmark European Union Court of Justice (CJEU) decision from 2014. The case revolved around the "right to be forgotten" and online privacy. In this case, a Spanish individual named Mario Costeja González requested that Google remove links to newspaper articles that contained information about his prior debts and property auction. He argued that the information was no longer relevant, and he wanted it to be "forgotten". Google, a search engine, was indexing and displaying these links in its search results. The CJEU ultimately ruled that, under certain circumstances, search engines like Google are considered data controllers and must respect the data subject's right to erasure or "right to be forgotten". This means that search engines can be required to remove or de-index specific search results containing personal information when requested by an individual, provided that the information is inadequate, irrelevant, or no longer necessary for the purposes of data processing. The Google Spain case set a significant precedent for online privacy and data protection in the European Union and had wide-reaching implications for how search engines and other online platforms handle personal data and privacy requests*).

name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be when its publication in itself on those pages is lawful".[449] Furthermore, the Court emphasized that the value of the data subject's right extends beyond the economic interests of the data controller and the public's interest in accessing the information.[450]

Data Controllers are responsible for ensuring the lawfulness of data processing, in accordance with the principle of accountability as outlined in Article 5, Paragraph 2. Consequently, controllers bear the burden of proving the legitimacy of data processing.[451]

In the wake of the judgement, the WP29 issued guidelines, which include a set of common criteria for implementing the CJEU ruling concerning the right to erasure.[452]

5. *The Right to Restriction of Processing*

As an alternative to the right to erasure, the GDPR also includes the right to restrict processing. A data subject can request the data controller to temporarily limit the processing of their personal data. Article 18, Paragraph 1 of the GDPR specifies the situations in which the data subject can request the controller to restrict processing: "*(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the per-*

[449] Ibid, Paragraph 62.

[450] Ibid., Paragraph 81.

[451] See, GDPR, Article 17.

[452] Article 29 Data Protection Working Party, *Guidelines on the implementation of the Court of Justice of the European Union Judgment on "Google Spain and Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, WP 225, of 26 November 2014.

sonal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject".

When personal data processing is restricted, personal data may be processed, except for storage, under certain circumstances. These circumstances include obtaining the data subject's consent, processing for the establishment, exercise, or defense of legal claims, protecting the rights of another natural or legal person, or for reasons of significant public interest within the Union or a Member State.

Controllers have the authority to restrict personal data, which can involve actions such as temporarily moving selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In the case of automated filing systems, the restriction should be enforced through technical means.[453]

Regarding the right to rectification, the right to erasure, and the right to restrict processing, as specified in Article 19 of the GDPR, the Controller is obligated to inform the data subject of any changes in data processing.

6. The Right to Data Portability

The is no legal precedent for data portability in the EU; it has thus been classified as a "brand new right".[454] The right to data portability allows data subjects to reuse their personal data for their own purposes when moving it from one controller to another.

---

[453] See, GDPR, Recital 67.

[454] L. Scudiero, *Bringing Your Data Everywhere: A Legal Reading of the Right to Portability*, European Data Protection Law Review, Vol. 2, Issue 1, 2017, page 119.

This right is provided for in the GDPR. Article 20 of the GDPR regulates the right to data portability, stating: "*The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means*". Recital 68 of the GDPR emphasizes that the right to data portability applies only in cases where personal data processing is based on consent or a contract.

The GDPR does not provide detailed guidance regarding the right to data portability; comprehensive guidelines were issued by the WP29.[455] According to the WP29 guidelines, the right to data portability "*supports user choice, user control, and user empowerment*". The key elements of data portability include the right of data subjects to receive personal data from the controller in a commonly used machine-readable format, the right to transmit this data to another controller without hindrance, the regime of controllership, and the exercise of the right to data portability without prejudice to any other rights.[456]

The concept of controllership entails that the data controller carries out the instructions of the data subject. Consequently, controllers are not responsible for ensuring the data subject recipient's compliance with data protection laws.[457]

---

[455] Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, WP 242 rev. 0.1, of 3 December 2016, Revised and adopted on 5 April 2017.

[456] Ibid.

[457] See, Council of Europe, Handbook on European data protection law, pages 228-229.

7. The Right to Object

The Right to Object, as established under the GDPR, empowers individuals to voice their concerns and dissent regarding the processing of their personal data. This fundamental right allows individuals to object to specific data processing activities, providing them with a degree of control over how their personal information is used. Whether it's for marketing purposes, automated decision-making, or other data processing activities, the right to object ensures that individuals can safeguard their privacy.

The right to object, outlined in Article 21 of the GDPR, is a fundamental component of data protection regulation. It provides data subjects with the ability to object to certain data processing activities in specific scenarios.

Four key situations for exercising the right to object are: 1) processing based on "particular situation": the right to object can be exercised when a data controller processes or profiles an individual's data, considering their "particular situation." According to the CJEU, the determination of what constitutes a "particular situation" is left to the national courts, and they assess the lawfulness and context of this situation. [458] This right to object seeks to strike a balance between the rights of the data subject and the legitimate interests of the data controller. Notably, in the case of Google Spain, the CJEU emphasized that fundamental rights take precedence over economic interests; 2) direct marketing means data subjects have the right to object to the use of their personal data for direct marketing purposes. This situation is known as the right to object to direct marketing.[459] Under the DPD, two possibilities were provided: firstly, data subjects could directly request the controller to stop processing their personal data for direct marketing, a right still

[458] See, Judgment of the CJEU, of 9 March 2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*, case C-398/15, ECLI:EU:C:2017:197.

[459] G. Zanfir-Fortuna, *Article 21. Right to object, in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020, page 510.

available today; secondly, data subjects could be informed by controllers before their personal data were made available to third parties for direct marketing. 3) automated processing for information society services: In cases where personal data is processed for information society services, data subjects can object to their data being processed automatically. 4) Scientific, Historical, or Statistical Research: data subjects can object to their data being used for research purposes, except when the research serves a public interest. The interpretation of scientific research under EU law is broad, encompassing privately funded research, technological development, fundamental research, genealogical purposes, and operations necessary for statistical surveys. It's important to note that the GDPR doesn't apply to the data of deceased persons. Therefore, the right to object may be limited to historical research.

According to Article 21 of the GDPR, when a data controller receives a request to exercise the right to object, they must cease data processing unless they can demonstrate the lawfulness of the processing.

The GDPR is built around the concept of "lawful processing" of data. That is, personal data cannot be processed unless a data controller has obtained individual consent, or the processing falls under one of the additional five listed categories of lawful processing.[460]

The right to object is a well-established right, as it is contained in the DPD, which all EU member states transposed into their national laws.[461]

8. The Right related to Automated Decision-Making including Profiling

Under the GDPR, the right related to automated decision-making, including profiling, is a fundamental aspect of personal data protection and privacy. This right

[460] V. Krishnamurthy, *Symposium on the GDPR and International law*, 2020.

[461] G. Zanfir-Fortuna, Article 21. Right to object, page 511.

is especially relevant in the context of AI and automated systems that make decisions about individuals without direct human intervention.

This right is detailed in Article 22, Paragraph 1 of the GDPR "*The data subject shall have the 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*". Furthermore, Article 22, Paragraph 2 clarifies that this right does not apply in situations where the automated decision-making is "*(a) necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent*".

Upon the GDPR coming into force, the WP29 provided further guidance on the use of automatic decision-making under the GDPR. It emphasizes that automated processing should be viewed as a general prohibition and data subjects do not need to proactively oppose such decisions.[462]

Scholar argues that automated decision-making without any human intervention or understanding challenges European ideas of autonomy and personality.[463] There is also significant debate about whether data subjects have a right to be informed in automatic decision-making processes.[464]

However, provisions in Articles 13, 14, 15, and 22 of the GDPR stipulate that the controller must provide data subjects with meaningful information about how their data is used. Specifically, Articles 13, Paragraph 2, letter f, and 14, Para-

---

[462] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making, and Profiling for the purposes of Regulation 2016/679*, WP 251 rev. 01, of 3 October 2017, and adopted on 6 February 2018.

[463] M. L. Jones, *The right to a human in the loop: Political constructions of computer automation and personhood*, Social Studies of Science, Vol. 47, No. 2, 2017.

[464] A. D. Selbst, and J. Powles, *Meaningful information and the right to explanation*, International Data Privacy Law, Vol. 7, No. 4, 2017.

graph 2, letter g, of the GDPR require data subjects to receive meaningful information about the logic involved and the envisaged consequences of automatic decision-making processing.

Chapter 3
The Rights of Information Subjects under the Chinese Civil Code and the PIPL

The Chinese Civil Code and the Chinese Personal Information Protection Law (PIPL) have introduced new rights to enhance the protection of information subjects. Before their enactment, the rights of information subjects were primarily governed by the General Provisions of the Chinese Civil Code and the Chinese Cybersecurity Law.

The Chinese Civil Code has supplanted the General Provisions of the Chinese Civil Code, and consequently, the rights of information subjects in China are now codified in the Chinese Civil Code, the Chinese Cybersecurity Law, and the Chinese PIPL.

1. The Rights of Information Subjects under the Chinese Civil Code

The Chinese Civil Code recognises the right to personal information protection and has shifted from a one-dimensional model to a dual-dimensional model, thereby distinguishing the right to privacy from the right to personal information as two distinct and autonomous rights.[465]

The Chinese Civil Code affirms that "*The processing of personal information shall be in compliance with the principles of lawfulness, justification, and within a necessary limit, and shall not be excessively processed*".[466]

Regarding the rights of information subject, Article 1037 of the Chinese Civil Code outlines various rights, including the right to access or to obtain a copy, the right to object, the right to rectify, and the right to delete. Specifically, it stipu-

[465] See, Part 2, Chapter 4, Paragraph 3.

[466] See, Article 1035 of the Chinese Civil Code; Translated by the National People's Congress (NPC), the original test is "处理个人信息的, 应当遵循合法, 正当, 必要原则, 不得过度处理".

lates, "*both parties while processing his personal information, he has the right to request the information processor to delete it in a timely manner both parties while processing his personal information, he has the right to request the information processor to delete it in a timely manner*".[467]

The Chinese Civil Code does not explicitly grant the right to be informed. However, Article 1035 stipulates that the rules governing personal information processing must be made publicly disclosed, with clear indications of the methods, purposes, and scope of information processing. The use of terms words "publicly disclosed" and "clear indications" signifies adherence to the transparency principle, indirectly acknowledging the information subject's right to be informed.[468]

2. The Rights of Information Subjects under the PIPL

Comparing the PIPL to the Chinese Civil Code, it becomes apparent that while the PIPL offers more detailed provisions, there is often redundancy with the rights stipulated in both the Chinese Civil Code and the PIPL.

A public debate in China among legal scholars on the nature of personal information rights.[469] Many Chinese scholars contend that the rights of information subjects are clearly delineated in the Civil Code, thus firmly placing them within the realm of civil law, a branch of private law. Conversely, other scholars argue

---

[467] Translated by the National People's Congress (NPC), the original test is "然人可以依法向信息处理者查阅或者复制其个人信息; 发现信息有错误的, 有权提出异议并请求及时采取更正等必要措施. 自然人发现信息处理者违反法律, 行政法规的规定或者双方的约定处理其个人信息的, 有权请求信息处理者及时删除".

[468] W. Huang, *中华人民共和国民法典人格权编解读, (Zhōnghuá rénmín gònghéguó mínfǎ diǎn réngé quán biān jiědú, Interpretation of Personality Rights in the Civil Code of the People's Republic of China)*, China Legal Publishing House, 2020, page 218.

[469] Guo, Chen, and Jia, *《个人信息保护法》 具体适用中的若干问题探讨 - 基于 《民法典》 与 《个人信息保护法》 关联的视角* (《Gèrén xìnxī bǎohù fǎ》 jùtǐ shìyòng zhōng de ruògān wèntí tàntǎo —jīyú 《mínfǎ diǎn》 yǔ 《gèrén xìnxī bǎohù fǎ》 guānlián de shìjiǎo).

that the PIPL also governs the rights of information subjects and can be applied in both the public and private law sectors. Therefore, making unequivocal claims about the exclusively private nature of these rights may be overly simplistic.[470] For instance, provisions pertaining to the protection of netizens often fall under the private sector, yet they may occasionally necessitate intervention by fundamental laws to safeguard these rights, which are part of the branch of public law.
Within the PIPL, various rights for information subjects are addressed. The PIPL covers the right to be informed, the right to access or request a copy of personal information, the right to information portability, the right to correct or supplement information, the right to object to automated decisions, and the right to request the deletion of personal data. Some of these rights have already been regulated by the Chinese Cybersecurity Law, such as the right to access, the right to delete, and the right to rectify.

a) The Right to Be Informed

According to the PIPL, individuals have the right to be informed about the processing of their information. This right is detailed in Article 17 of the PIPL, which states: "*A personal information processor shall, before processing personal information, truthfully, accurately and fully inform an individual of the following matters in a easy-to-notice manner and in clear and easy-to-understand language: (1) the name and contact information of the personal information processor; (2) the purposes and means of personal information processing, and the categories and storage periods of the personal information to be processed; (3) the methods and procedures for the individual to exercise his rights as provided in*

[470] J. Yao, *System of rights of personal information subjects (个人信息主体的权利体系-基于数字时代个体权利的多维观, Gèrén xìnxī zhǔtǐ de quánlì tǐxì)*, Journal of East China University of Political Science and Law (华东政法大学学报, Huádōng zhèngfǎ dàxué xuébào), No. 2, 2022.

this Law; and (4) other matters that the individual should be notified of as provided by laws and administrative regulations. Where any matter as set forth in the preceding paragraph changes, the individual shall be informed of the change. Where the personal information processor informs an individual of the matters specified in the first paragraph by formulating personal information processing rules, the processing rules shall be made public and be easy to consult and save".[471]

The right to be informed has limitations, as defined in Article 18 of the PIPL, which states: "*When processing personal information, personal information processors are permitted not to inform individuals of the matters specified in the first paragraph of the preceding article where laws or administrative regulations require confidentiality or provide no requirement for such notification. Where it is impossible to notify individuals in a timely manner in a bid to protect natural persons' life, health and property safety in case of emergency, the personal information processors shall notify them without delay after the emergency is removed.*".[472]

---

[471] Translated by the National People's Congress (NPC), the original text is "个人信息处理者在处理个人信息前, 应当以显著方式, 清晰易懂的语言真实, 准确, 完整地向个人告知下列事项: （一）个人信息处理者的名称或者姓名和联系方式; （二）个人信息的处理目的, 处理方式, 处理的个人信息种类, 保存期限; （三）个人行使本法规定权利的方式和程序; （四）法律, 行政法规规定应当告知的其他事项. 前款规定事项发生变更的, 应当将变更部分告知个人. 个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的, 处理规则应当公开, 并且便于查阅和保存".

[472] Translated by the National People's Congress (NPC), the original text is "个人信息处理者处理个人信息, 有法律, 行政法规规定应当保密或者不需要告知的情形的, 可以不向个人告知前条第一款规定的事项. 紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的, 个人信息处理者应当在紧急情况消除后及时告知".

b) The Right to Access or Obtain a Copy

The right of access is one of the earliest rights to appear in the primary legal instruments related to personal information protection.[473] The right to access, or to obtain a copy of personal information, is outlined in Article 45, Paragraphs 1 and 2 of the PIPL, which states, "*Individuals shall have the right to consult and duplicate their personal information from personal information processors, except under circumstances as set out in the first paragraph of Article 18 and Article 35 of this Law. Where an individual requests the consultation or duplication of his personal information, the requested personal information processor shall provide such information in a timely manner*".[474]

In the Chinese legal system, the right to access includes the right to obtain a copy of personal information.

The personal information processor should furnish details regarding the methods, purposes, and storage of the personal information. Only by having access to this information can individuals determine whether the processing of their information aligns with their interests.

c) The Right to Information Portability

Article 45, Paragraph 3 of the PIPL addresses the novel concept of information portability, stating, "*Where an individual requests the transfer of his personal information to a designated personal information processor, which meets the requirements of national cyberspace department for transferring personal infor-*

[473] Shen, On the Construction and Systematization of the Personal Information Right (论个人信息权的构建及其体系化), page 6.

[474] Translated by the National People's Congress (NPC), the original text is "个人有权向个人信息处理者查阅, 复制其个人信息; 有本法第十八条第一款, 第三十五条规定情形的除外. 个人请求查阅, 复制其个人信息的, 个人信息处理者应当及时提供".

mation, the requested personal information processor shall provide means for the transfer".[475]

This marks the first instance of the Chinese legislator introducing the right to information portability into the Chinese legal system. In fact, it was a subject of controversy in the first two draft versions of the PIPL.[476]

d) The Right to Correct or Supplement

When the personal information contains errors, is inaccurate, or is incomplete, the information subject has the right to request the correction or supplementation of their personal information. Article 46 of the PIPL explicitly states, "*Where an individual discovers that his personal information is incorrect or incomplete, he shall have the right to request the personal information processors to rectify or supplement relevant information. Where an individual requests the rectification or supplementation of his personal information, the personal information processors shall verify the information in question, and make rectification or supplementation in a timely manner*".[477]

[475] Translated by the National People's Congress (NPC), the original text is "个人请求将个人信息转移至其指定的个人信息处理者, 符合国家网信部门规定条件的, 个人信息处理者应当提供转移的途径".

[476] Shen, On the Construction and Systematization of the Personal Information Right (论个人信息权的构建及其体系化), pages 7-8.

[477] Translated by the National People's Congress (NPC), the original text is "个人发现其个人信息不准确或者不完整的, 有权请求个人信息处理者更正, 补充. 个人请求更正, 补充其个人信息的, 个人信息处理者应当对其个人信息予以核实, 并及时更正, 补充".

e) The Right to Object relating to Automated Decisions

Article 24 of the PIPL, Paragraph 3, introduced a new information subject right into the Chinese legal system, which is the right to object in relation to automated decisions.

Article 24 of the PIPL, Paragraphs 1 and 2 stipulate, "*Personal information processors using personal information for automated decision making shall ensure the transparency of the decision making and the fairness and impartiality of the results, and may not apply unreasonable differential treatment to individuals in terms of transaction prices and other transaction conditions. Information push and commercial marketing to individuals based on automated decision making shall be simultaneously accompanied by options not specific to their personal characteristics or with convenient means for individuals to refuse*".[478] Paragraph 3 establishes the right to object in relation to automated decisions, allowing "*the individual shall have the right to request clarification from the personal information processor and the right to refuse the processor for making the decision only through automated decision making*".[479]

The right to object can be exercised in two specific situations: firstly, in processes related to business marketing purposes, and secondly, when the automated process has a significant impact on the rights and interests of the information subject.

[478] Translated by the National People's Congress (NPC), the original text is "个人信息处理者利用个人信息进行自动化决策, 应当保证决策的透明度和结果公平, 公正, 不得对个人在交易价格等交易条件上实行不合理的差别待遇. 通过自动化决策方式向个人进行信息推送, 商业营销, 应当同时提供不针对其个人特征的选项, 或者向个人提供便捷的拒绝方式".

[479] Translated by the National People's Congress (NPC), the original text is "通过自动化决策方式作出对个人权益有重大影响的决定, 个人有权要求个人信息处理者予以说明, 并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定".

f) The Right to Delete

Article 47 of the PIPL aims to refine the right to deletion, building upon the concept provided by the Chinese Civil Code. It delineates five situations in which the information subject can exercise their right to deletion: "*(1) the purposes of processing have been achieved or cannot be achieved, or such information is no longer necessary for achieving the purposes of processing; (2) the personal information processor ceases to provide products or services, or the storage period has expired; (3) the individual withdraws his consent; (4) the personal information processor processes personal information in violation of laws, administrative regulations, or agreements; or (5) other circumstances as provided by laws and administrative regulations*".[480]

Regarding the right to delete, TC26 underscores that when a user requests the permanent deletion of their account, personal information processors providing goods or services must immediately delete or anonymize the personal information upon account deletion, or within 15 days if manual processing is required. When sensitive information is involved, the relevant provisions on sensitive information must be adhered to.[481]

Lastly, Article 49 of the PIPL acknowledges the right of access, the right to obtain a copy of personal information, the right to rectify, and the right to delete for the

---

[480] Translated by the National People's Congress (NPC), the original text is "（一）处理目的已实现, 无法实现或者为实现处理目的不再必要; （二）个人信息处理者停止提供产品或者服务, 或者保存期限已届满; （三）个人撤回同意; （四）个人信息处理者违反法律, 行政法规或者违反约定处理个人信息; （五）法律, 行政法规规定的其他情形".

[481] Zhōnghuá rénmín gònghéguó guójiā shìchǎng jiāndū guǎnlǐ zǒngjú (中华人民共和国国家市场监督管理总局, State Administration for Market Supervision of the People's Republic of China), and Zhōngguó guójiā biāozhǔnhuà guǎnlǐ wěiyuánhuì (中国国家标准化管理委员会, Standardization Administration of the People's Republic of China), Information Security Technology-Personal Information Security Specification, GB/T 35273-2017, of 29 December 2017, page 14.

family members of a deceased individual, unless the deceased had expressed a different preference before their passing.

Conclusion of Part 4

The International and EU legal systems, particularly the GDPR have influenced the formation of the rights of Information Subject in the Chinese legal system, particularly the PIPL. Between the EU and Chinese legal systems, the rights of data/information subjects, such as the right to be informed, the right to restriction of processing, the right to rectify and supplement, called in the GDPR the right to rectification, and the right of access are quite similar, with some differences in the right to object, the right relating to automated decision-making, and the right to delete.

The concept of the right to object in the GDPR comparing the concept in the Chinese legal system is wider as well as the right relating to automated decision-making. In the PIPL the right to object can exercise only in the automatic personal information process case. Automatic decision-making including profiling in China is still developing. For instance, the PIPL and other laws do not provide the form to exercise the right to object to information subject and do not explain the technical requirement to ensure the personal information.

The biggest difference is the right to delete, called the right to erasure from the international and EU law sides.

The right to erasure also includes the right to be forgotten. According to Article 17 of the GDPR can request to erasure their personal data, with the only legal limit, under Paragraph 3 of the same Article. Instead, the right to delete, in the Chinese legal system does not recognize the right to be forgotten, and the right to delete can exercise when there is a violation of the personal information subject, and the situations provided by Article 47 of the PIPL. Some scholars have stated that the right to delete in the Chinese legal system as it is structured is not a right for information subject, but rather a request to the personal information processor.[482]

---

[482] L. Wang, Lùn gèrén xìnxī shānchú quán (论个人信息删除权, On the right to delete personal information), Oriental Law (东方法学), No. 1, 2022, pages 39-42.

PART 5
THE ENFORCEMENT OF PERSONAL DATA PROTECTION LEGAL STANDARDS

The enforcement of personal data protection standards plays a pivotal role in ensuring the effective application of rules and regulations. It is critical to regulate personal data transfer and the infringements of personal data, as these are two essential enforcement components.

In our contemporary globalized society, the transfer of personal data has become a common occurrence, particularly in the online realm, owing to the borderless nature of the virtual environment. Consequently, the personal data of netizens is increasingly vulnerable to various risks. While the transfer of personal data promotes the principles of free data flow, it is imperative to establish robust safeguards to protect the rights and freedoms of data subjects. This transfer of personal data has drawn significant attention from both legislators and economic operators, given its significant role in the processing of personal data. Concurrently, the sanctions outlined for breaches in personal data processing hold paramount interest and significance, as they define the immediate consequences of personal data violations.

This part will delve into the legal standards governing the transfer of data to third countries and international organizations, along with the penalties established for violations in personal data processing. It is structured into two Chapters. The first Chapter addresses the rules governing data transfers within the international legal systems of the EU and China, while the second Chapter analyzes the sanctions specified by legislators in the international legal systems of the EU and China in the event of infringements of personal data.

Chapter 1
The Cross-Border Transfer of Personal Data in International, EU, and Chinese Legal Systems

Personal data transfer means the deliberate act of sending personal data to another party or granting access to the data, where neither the sender nor the recipient qualifies as a data subject. It is crucial to clarify that data transfer should not be confused with personal data collection.[483]

In the international context, the transfer of personal data is the subject of several international treaties. For instance, the Umbrella Agreement,[484] the international agreements between the EU and Canada,[485] Australia.[486] The primary multilateral

[483] Personal data collection refers to the process of gathering, storing, or obtaining information about individuals or subjects that can be used to identify, describe, or categorize them. This data can include a wide range of information, such as names, addresses, phone numbers, email addresses, social security numbers, financial records, photographs, and any other details that can be linked to a specific person. The collection of personal data can occur through various means, including online forms, surveys, interviews, surveillance, and more, and it's often conducted by organizations or entities for various purposes, such as research, marketing, or administrative needs. It's important for organizations to handle personal data collection in compliance with relevant data protection and privacy regulations to ensure the rights and privacy of individuals are respected. In summary, personal data collection is the initial process of gathering information about individuals, while the transfer of personal data involves sending or sharing that collected data with other parties or granting access to it for specific purposes.

[484] The "Umbrella Agreement" is an international treaty that establishes a framework for the protection of personal data exchanged between the European Union (EU) and the United States for law enforcement purposes. It aims to ensure that personal data transferred for criminal investigations and law enforcement cooperation is subject to strong data protection and privacy safeguards. The agreement sets standards for data security, access, and redress mechanisms for individuals whose data is transferred, contributing to the protection of fundamental rights in transatlantic law enforcement cooperation.

[485] The Passenger Name Record (PNR) Agreement between the European Union (EU) and Canada, signed in 2006, facilitates the exchange of airline passenger data for the purposes of enhancing

agreement relevant to international personal data transfer remains the Convention 108 of the Council of Europe.
In the EU law, the provision is more direct and concise, it was previously part of the DPD, and has now been replaced by the GDPR. A similar situation exists in the Chinese context, where the provision is outlined in the PIPL.

1. The Cross-Border Transfer of Personal Data under Convention 108

Convention 108 is the primary international legal instrument for the transfer of personal data. It is supplemented by an Additional Protocol.[487]
The Additional Protocol to Convention 108, adopted in 2001, extends the protections of the original convention by addressing the international transfer of personal data and reinforcing the rights and privacy of individuals when their data is transferred across borders. It emphasizes data security, notification, and data subject rights in the context of transborder data flows.
In the context of transborder data flows, the protocol addresses the transfer of personal data across borders, emphasizing the need for protection, even when data is

---

aviation security and law enforcement cooperation. It establishes data protection safeguards, outlines data usage restrictions, sets retention periods, and provides redress mechanisms for individuals. The agreement fosters collaboration between the EU and Canada, enabling the balanced management of security and privacy considerations in international air travel.

[486] The Passenger Name Record (PNR) Agreement between the European Union (EU) and Australia, signed in 2012, allows the exchange of airline passenger data for enhancing aviation security and combating transnational crime, including terrorism. It includes data protection provisions, limiting data use to security and law enforcement purposes, defining retention periods, and offering redress mechanisms for individuals. This agreement serves as a framework for cooperation between the EU and Australia to balance security and privacy concerns in the context of international air travel.

[487] Council of Europe, European Treaty Series - No. 181, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, 8 November 2001.

transferred to countries outside the jurisdiction of the original data protection laws. Specifically, Article 2, Paragraph 1 of the Additional Protocol states that "*Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer*". Additionally, Paragraph 2 allows for derogations when: "*a) domestic law provides for it because of specific interests of the data subject, or legitimate prevailing interests, especially important public interests; or b) safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law*".

Similar rules are also found in the Modernized Convention 108. Article 14, Paragraph 1 states that "*A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so if bound by harmonised rules of protection shared by States belonging to a regional international organisation*". Paragraph 2 specifies that "*When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured*". According to Paragraph 3, this appropriate level of protection can be achieved through "*the law of that State or international organisation, including the applicable international treaties or agreements; or ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing*". Additionally, Paragraph 4 outlines four situation where the transfer of personal data can take place: "*a) the data subject has given explicit, specific and*

free consent, after being informed of risks arising in the absence of appropriate safeguards; or b) the specific interests of the data subject require it in the particular case; or c) prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; or d) it constitutes a necessary and proportionate measure in a democratic society for freedom of expression". These situations represent derogation to international data transfers.[488]

Finally, Article 15 states that each Party must provide the competent supervisory authority with all information relevant to data transfers and has the right to request "*that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to condition*".

2. The Cross-Border Transfer of Personal Data under the GDPR

The EU Commission initiated studies on the regulation of trans-border personal data flows in 1973.[489] This action was prompted by cases in which the free flow of data between the Member States of the European Communities faced threats due to varying levels of data protection applicable in those states.[490] For instance, in 1980, an Austrian government ordinance required prior authorization from the Austrian Data Protection Commission before the transfer of personal data of legal

---

[488] C. Kuner, *Article 49. Derogations for specific situations, in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020, page 845.

[489] H. Mengel, *Internationale Organisationen und transnationaler Datenschutz: Einführung und Dokumentation*, Wissenschaftlicher Autoren-Verlag, 1984.

[490] C. Kuner, *Article 44, General principle for transfer, in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020, page 758.

persons to France, Germany, or Sweden.[491] This was because the data protection laws in those countries did not encompass such data. During the 1970s, the Swedish Data Protection Board consistently denied authorization for the transfer of personal data to the United Kingdom in several cases.[492] In 1989, the French subsidiary of the Italian automobile company Fiat was permitted by the French data protection authority to transfer employee data to Italy only after a data transfer agreement was signed between the two companies. This was due to the absence of data protection legislation in Italy at the time.[493]

Before the GDPR came into effect, the regulations governing the transfer of personal data were outlined in Articles 25 and 26 of the DPD. Today, these similar provisions can be found in Chapter V, specifically in Articles 44 through 50 of the GDPR.

Article 44 of the GDPR sets out the fundamental principle that governs the transfer of personal data to third countries or international organizations. It emphasizes that "*Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined*".

---

[491] Austrian Regulation on Equivalence 1980, Verordnung des Bundeskanzlers vom 18, über die Gleichwertigkeit ausländischer Datenschutzbestimmungen, BGBl II Nr. 612/ 3403, December 1980.

[492] J. Bing, *Transnational Data flows and the Scandinavian Data Protection Legislation*, Scandinavian studies in law 24 1980, October 1980, page 73.

[493] Commission nationale de l'informatique et des libertés (CNIL), 10e rapport d'activité, 1989, page 32.

Articles 45 and 46 specify that if the transfer is authorized by EU law or meets the adequacy requirements for data protection, the transfer can occur without the need for specific authorizations. In cases where adequacy is not met, the data controller or processor may transfer the data to a third country or international organization only after providing appropriate safeguards. These safeguards may include legally binding instruments, binding corporate rules, standard data protection clauses, approved codes of conduct, or certified mechanisms. Ensuring the rights and remedies of data subjects remains of paramount importance.

Article 47 explains the concept of binding corporate rules, which is a mechanism for multinational corporations to transfer data within their group of undertakings while ensuring data protection. These rules must be legally binding, provide enforceable rights to data subjects, and comply with specific requirements. Approval by the competent supervisory authority is mandatory. Binding corporate rules enable organizations to maintain consistent data protection standards across their global operations.

In contrast, Article 48 regulates the situation of the transfer of personal data not authorized by EU law, stating that "*Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter*". Agreements on trans-border transfer of personal data could help resolve some of the conflicts of law.[494]

To complete this framework, Article 49 outlines derogations or exceptions that allow the transfer of personal data to third countries or international organizations in

[494] T. Christakis, *Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?*, Randal Milch and Sebastian Benthall (eds), "Cybersecurity and Privacy in a Globalized World - Building Common Approaches", New York University School of Law, e-book (Forthcoming), 14 June 2019.

specific situations. These situations include explicit consent, the performance of a contract, vital interests, legal claims, and the protection of public interests. If none of the provisions in Articles 45 or 46 apply, a transfer may occur under certain conditions, provided that the data controller assesses and safeguards the data.
Finally, Article 50 emphasizes the critical role of international cooperation in the enforcement of data protection legislation. It calls for the development of effective enforcement mechanisms, mutual assistance, engagement with stakeholders, and the exchange of information concerning personal data protection. This article acknowledges that collaboration between the EU and third countries is indispensable for safeguarding personal data in the global context. Notably, the DPD did not include a provision equivalent to this.[495]

3. The Cross-border Transfer of Personal Information under the PIPL

Transferring personal information outside the borders of China is subject to Article 38 of the PIPL, which states that "*A personal information processor that truly needs to provide personal information for a party outside the territory of the People's Republic of China for business sake or other reasons, shall meet one of the following requirements: (1) passing the security assessment organized by the national cyberspace department in accordance with Article 40 of this Law; (2) obtaining personal information protection certification from the relevant specialized institution according to the provisions issued by the national cyberspace department; (3) concluding a contract stipulating both parties' rights and obligations with the overseas recipient in accordance with the standard contract formulated by the national cyberspace department; and (4) meeting other conditions set forth*

[495] C. Kuner, *Article 50. International cooperation for the protection of personal data, in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020, page 859.

by laws and administrative regulations and by the national cyberspace department".[496]

Additionally, according to Article 39 of the PIPL "*Where a personal information processor provides personal information for any party outside the territory of the People's Republic of China, the processor shall inform the individuals of the overseas recipient's name and contact information, the purposes and means of processing, the categories of personal information to be processed, as well as the methods and procedures for the individuals to exercise their rights as provided in this Law over the overseas recipient, etc., and shall obtain individual's separate consent*".[497]

Moreover, Article 40 of the PIPL stipulates that, when transferring significant amounts of personal information, information handlers are required to request a security assessment from the Chinese State Cybersecurity and Informatization Department. This emphasizes the crucial role of the Chinese Government in regulating cross-border personal information transfers.[498]

Recent developments in China's personal information protection landscape have led to significant changes in the context of cross-border data transfers, particularly under the PIPL.

---

[496] Translated by the National People's Congress (NPC), the original text is "个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；（四）法律、行政法规或者国家网信部门规定的其他条件".

[497] Translated by the National People's Congress (NPC), the original text is "向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意".

[498] D. Xie, *个人信息跨境提供中的企业合规 (Gèrén xìnxī kuà jìng tígōng zhōng de qǐyè hé guī, On the Corporate Compliance in Cross-border Supply of Personal Information)*, 法学论坛 (Fǎxué lùntán, Legal Forum), 2023, page 1.

In February 2023, the Cyberspace Administration of China introduced rules governing Standard Contractual Clauses (PIPL SCCs) for the transfer of personal information to third countries, adding to the trio of established mechanisms for such transfers. These PIPL SCCs rules came into effect on June 1, 2023.[499]

The PIPL SCCs state that personal information processors can transfer personal information outside of China by entering a standard contract for the transfer of personal information with the overseas recipient.[500] Before PIPL SCCs came into force, in China, transferring personal information outside of China required compliance with Article 38 of the PIPL. Now, there is an additional option, if personal information processors meet one of the conditions specified in Article 4 of the PIPL SCCs, they can transfer personal information without undergoing a security assessment. According to Article 4, "*Personal information processors that provide personal information overseas by entering into standard contracts must meet the following circumstances at the same time: (1) Non-critical information infrastructure operators; (2) Processing personal information of less than 1 million people; (3) The total number of personal information provided to overseas parties since January 1 of the previous year is less than 100,000; (4) The cumulative number of sensitive personal information provided to overseas parties since January 1 of the previous year is less than 10,000*".[501] Non-critical Information Infrastructure Operator is broadly defined to include businesses in the financial, ener-

---

[499] 中华人民共和国国家互联网信息办公室 （Zhōnghuá rénmín gònghéguó guójiā hùliánwǎng xìnxī bàngōngshì, Cyberspace Administration of China）, 国家互联网信息办公室令第 13 号 (Guójiā hùliánwǎng xìnxī bàngōngshì lìng dì 13 hào, Cyberspace Administration of China Act No. 13), 个人信息出境标准合同办法 (Gèrén xìnxī chūjìng biāozhǔn hétóng bànfǎ, Standard Contract Measures for the Transfer of Personal Information Abroad), 22 February 2023.

[500] See, PIPL SCCs, Article 2.

[501] Translated by the author, the original text is "个人信息处理者通过订立标准合同的方式向境外提供个人信息的, 应当同时符合下列情形: (一) 非关键信息基础设施运营者; (二) 处理个人信息不满 100 万人的; (三) 自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的; (四) 自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的".

gy, telecom, public utility, healthcare, transportation, and other entities that are important to China's national security and welfare.

Chapter 2
The Infringement of Personal Data Law in International, EU, and Chinese Legal Systems

This Chapter delves into the intricate landscape of personal data breaches and the corresponding provisions governing such infringements. With a primary focus on the legal systems of international, EU, and China, we embark on an exploration of the multifaceted guidelines and penalties established to address these violations of personal data protection laws.

This Chapter is structured into three distinct Paragraphs. The first Paragraph delves into the realm of infringements under Convention 108, shedding light on the provisions it lays out. The second Paragraph shifts the spotlight to the infringements under the GDPR, offering an in-depth examination of its regulations. In the final part, the Paragraph dives into the infringements outlined in the PIPL.

The overarching aim of this Chapter is to provide a comprehensive understanding of the sanctions imposed in response to personal data breaches within the international, EU, and Chinese legal frameworks.

1. Sanctions for Infringement of Convention 108

Article 7 of the Modernised Convention 108 states that "*Each Party shall provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. Each Party shall provide that the controller notifies, without delay, at least the competent supervisory authority within the meaning of Article 15 of this Convention of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects*".

Article 10 of Convention 108 mandates that Contracting Parties must establish "*appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter*". Furthermore, Article 12 of the Modernised Convention 108 imposes an obligation on Contracting Parties to establish "*appropriate judicial and non-judicial sanctions and remedies for violations of the provisions of this Convention*".
It is worth noting that neither of these two articles provides specific details regarding the provisions under national law.[502]

2. Sanctions for Infringement of the GDPR

In EU law, particularly under the GDPR, the provisions related to cases of infringement due to personal data breaches are intricate. For instance, data subjects have several rights and options, including the right to lodge a complaint with a supervisory authority,[503] the right to an effective judicial remedy against a supervisory authority,[504] controller or processor,[505] the right to mandate,[506] suspension of proceedings,[507] the right to compensation and liability.[508]
Regarding the right to compensation, as articulated in Article 82, Paragraph 1, it stipulates that "*Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered*".

---

[502] W. Kotschy, *Art. 83. General conditions for imposing administrative fines, in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020, page 1186.

[503] See, GDPR, Article 77.

[504] See, GDPR, Article 78.

[505] See, GDPR, Article 79.

[506] See, GDPR, Article 80.

[507] See, GDPR, Article 81.

[508] See, GDPR, Article 82.

Under the GDPR, in the event of a GDPR infringement, there are two types of penalties: administrative fines and "other" penalties, which are applicable to infringements not subject to administrative fines.

Administrative fines are regulated in Article 83 of the GDPR. This article outlines a series of considerations that must be considered when determining the amount of an administrative fine. These considerations include: "*(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; (b) the intentional or negligent character of the infringement; (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects; (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32; (e) any relevant previous infringements by the controller or processor; (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; (g) the categories of personal data affected by the infringement; (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement; (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement*". The following Paragraphs of Article 83 establish specific limits regarding the amount of administrative fines that can be imposed for GDPR violations. These limits are categorized as follows: Paragraph 4 states "*Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to*

2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; (b) the obligations of the certification body pursuant to Articles 42 and 43; (c) the obligations of the monitoring body pursuant to Article 41(4)"; Paragraph 5 notes "*Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; (b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; (d) any obligations pursuant to Member State law adopted under Chapter IX; (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1)*"; and Paragraph 6 specifies "*Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher*".

Regarding "other" penalties, this provision is contained in Article 84 of the GDPR. According to Article 84, Paragraph 1, "other" penalties refer to infringements "are not subject to administrative fines pursuant to Article 83", and are determined by the Member States. In addition, Paragraph 2 states that "*Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them*".

Before the GDPR came into effect, penalties were governed by the DPD. The DPD is a directive and as such, the sanctions were provided for in the national

laws of the Member States concerning infringements of EU personal data protection.[509]

3. *Sanctions for Infringement of the PIPL*

The consequences of infringing the PIPL are very severe and could potentially lead to criminal liability and a curtailment of personal freedom. For example, Article 67 of the PIPL states "*Any violation of the provisions of this Law shall be entered in the relevant credit record and be published in accordance with the provisions of the relevant laws and administrative regulations*".[510]

The regulation of PIPL infringements is governed by Chapter 7, encompassing Articles 66 to 71 of the PIPL. In particular, Article 66 states, in cases "*Where personal information is processed in violation of the provisions of this Law or without fulfilling the personal information protection obligations provided in this Law, the departments with personal information protection duties shall order the violator to make corrections, give a warning, confiscate the illegal gains, and order the suspension or termination of provision of services by the applications that illegally process personal information; where the violator refuses to make corrections, a fine of not more than RMB one million yuan shall be imposed thereupon; and the directly liable persons in charge and other directly liable persons shall each be fined not less than RMB 10,000 yuan nor more than RMB 100,000 yuan. In case of an illegal act as prescribed in the preceding paragraph and the circumstances are serious, the departments with personal information protection duties at or above the provincial level shall order the violator to make corrections, confiscate the illegal gains, impose a fine of not more than RMB 50 million yuan or not more than five percent of the previous year's turnover; may also order the suspension of relevant businesses, or order the suspension of all the business operations for an*

[509] Kotschy, Art. 83. General conditions for imposing administrative fines, page 1184.

[510] Translated by the National People's Congress (NPC), the original text is "有本法规定的违法行为的, 依照有关法律, 行政法规的规定记入信用档案, 并予以公示".

overhaul, and notify the competent authorities to revoke relevant business permits or license; shall impose a fine of not less than RMB 100,000 yuan but not more than RMB 1 million yuan upon each of the directly liable persons in charge and other directly liable persons, and may decide to prohibit the abovementioned persons from serving as directors, supervisors, senior managers, or the persons in charge of relevant companies within a specific period of time.".[511]

[511] Translated by the National People's Congress (NPC), the original text is "反本法规定处理个人信息, 或者处理个人信息未履行本法规定的个人信息保护义务的, 由履行个人信息保护职责的部门责令改正, 给予警告, 没收违法所得, 对违法处理个人信息的应用程序, 责令暂停或者终止提供服务; 拒不改正的, 并处一百万元以下罚款; 对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款. 有前款规定的违法行为, 情节严重的, 由省级以上履行个人信息保护职责的部门责令改正, 没收违法所得, 并处五千万元以下或者上一年度营业额百分之五以下罚款, 并可以责令暂停相关业务或者停业整顿, 通报有关主管部门吊销相关业务许可或者吊销营业执照; 对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款, 并可以决定禁止其在一定期限内担任相关企业的董事, 监事, 高级管理人员和个人信息保护负责人".

Conclusion of Part 5

In conclusion, this part has offered a comparative perspective on personal data transfers under Convention 108, GDPR, and the PIPL, while also delving into the consequences of infringements within these frameworks.

The GDPR, as exemplified through Articles 44 to 50, presents a robust and comprehensive framework for international data transfers, underscoring the EU's unwavering commitment to data protection and privacy. The GDPR's emphasis on adequacy decisions, appropriate safeguards, and specific derogations forms a vital foundation for data security during cross-border exchanges. Additionally, binding corporate rules and international cooperation mechanisms play pivotal roles in facilitating global data flows while maintaining the highest standards of data protection. In essence, the GDPR sets a gold standard for personal data protection in international transfers, reinforcing the EU's role as a global leader in this domain.

It's worth noting that the PIPL SCCs, akin to the GDPR's SCCs, outline specific obligations for Personal Information Processors and overseas recipients. These obligations aim to ensure the secure and responsible transfer of personal information.

The GDPR's stringent personal data regulations, particularly in reporting data breaches within 72 hours, stand in contrast to the Data Protection Directive. GDPR streamlines and standardises data breach notification processes, promoting consistency and transparency across the EU.[512]

However, it's essential to recognize the comprehensiveness of provisions related to personal data breaches under the GDPR compared to Convention 108.

In terms of consequences for infringements, the PIPL imposes exceptionally serious penalties compared to both the GDPR and Convention 108, further underlining China's commitment to personal information protection and the severe repercussions for non-compliance.

---

[512] See, GDPR, Recital 85.

In addition to sanctions, in the event of a personal data breach, both the GDPR and the PIPL provide for the right to compensation under Article 82 of the GDPR and Article 69 of the PIPL.

This Part's comparative analysis highlights the unique strengths and focal points of each legal framework, offering a rich understanding of their contributions to the global landscape of personal data protection and data transfer regulations. The Part also underscores the critical importance of abiding by these regulations in an era where data is a driving force, and privacy and personal data protection and security are paramount.

CONCLUSION

In the culmination of this thesis, an exploration spanning the realms of personal data protection within the international, European Union (EU), and Chinese legal systems is unveiled. The journey embarked upon sought to navigate the intricate labyrinth of safeguarding personal data or information across these divergent but interconnected legal landscapes.

Recognising the immense expanse of the virtual world, this thesis extended its lens to encompass a comparative examination of three legal systems: international, EU, and Chinese.

At the heart of this thesis lay a fundamental question – how do we protect personal data or information in an era of accelerating technological advancement and global interconnectivity? The pursuit of an answer to this question unveiled a multifaceted narrative that traversed diverse legal frameworks, each offering its distinct perspective on the protection of personal data.

First and foremost, the research underscored a fundamental paradox in the field of personal data protection. International legal instruments, exemplified by the OECD guidelines and Convention 108, once considered beacons of protection, have fallen into obsolescence in the face of the swiftly evolving social and technological context. The modernisation efforts for Convention 108 in 2018, though commendable, could not keep pace with the relentless march of technology. Nevertheless, the legacy of these international instruments endures, having undoubtedly shaped the formation of the EU's legal apparatus for data protection.

Turning to the context of China, it is evident that the legal framework is in its nascent stages compared to the international and EU legal orders. The Chinese Personal Information Protection Law (PIPL) has garnered comparisons to the EU's General Data Protection Regulation (GDPR), earning the moniker of the “Chinese GDPR”.

The resemblance is unmistakable, yet the PIPL introduces distinctive elements. Notably, the PIPL places greater emphasis on the location of the personal information processing activity, while the GDPR primarily considers the location where the business is established.

This fusion of influences and distinctiveness echoes the dynamic nature of the PIPL. It reveals a law shaped not only by the GDPR but also by a multitude of international legal instruments on personal data protection. The Chinese government's assertion that the PIPL draws from global experiences while embracing its unique Chinese characteristics reflects the adaptability and flexibility that is emblematic of the evolving legal landscape.

As this thesis navigated the intricacies of personal data protection, it offered an exhaustive analysis, spanning the source of law, the imposition of sanctions in case of infringement, the subtleties of terminology between “data” and “information”, the nuances of the consent of data subjects, and the rights of data subjects.

This exploration unveiled intriguing divergences, such as the linguistic distinctions between “personal data” in Convention 108 and the EU legal system versus “personal information” in the Chinese legal framework. Despite these linguistic nuances, the core concept remains congruent. Furthermore, the concept of the consent of data subjects, while a common thread in all three legal systems, exhibited variations. The international and EU systems shared common ground in their approach, whereas the Chinese legal framework introduced the concept of both general and separate consent. Chinese separate consent aligns with the EU's concept of consent, but in Chinese law, it is specifically prescribed for certain cases stipulated by the law. In contrast, the EU typically expects a consent as the norm. The differences in these approaches underscore the intricacies and subtleties within the domain of personal data protection. Consent, in particular, is often subject to legal doctrine, leading to a scenario where it becomes a mere procedural formality to which the concerned party adheres without full awareness. This situation prompts inquiries into the genuine effectiveness of consent as a tool for safeguard-

ing individuals' rights in our progressively digitalized world. Exploring alternative strategies may become imperative, including streamlining privacy notices, embracing technological solutions that enhance comprehension of consent, or launching educational initiatives to elevate citizens' awareness of their digital rights. Similarly, in the case of the responsibility of data controllers to verify the age declared by users, practical implementation of these verification measures can be challenging.

Another matter of the thesis, the complex dynamics of data transfer was brought into focus. International law, in this regard, was observed to adopt a broader and more generic stance compared to EU law, which demonstrated detailed provisions. The PIPL has a more stringent framework compared to the GDPR. Despite these differences, a unanimous commitment to sanctions for personal data protection infringements, along with the provision for compensation for damages in both the EU and China.

As it has been said several times, technology is rapidly developing. To have perfect regulation in the protection of personal data remains elusive, as technological advances perpetually outstrip the legislative process. However, the imperative of synchronizing rules with the contemporary social context serves as a beacon, guiding the evolution of personal data protection.

As technology continues its inexorable march, the spectre of artificial intelligence (AI) looms large on the horizon. The EU and China are actively sculpting regulations tailored to the intricacies of AI. The EU's AI Act, set to come into force, holds the promise of being the first AI law worldwide. The interface of AI with personal data protection in the EU, particularly through the prism of Article 22 of the GDPR, underscores the imperative of aligning AI and data protection regulations.

The thesis emphasises that the advent of AI is not a distant spectre but an imminent reality, as evidenced by a recent incident in China involving the exploitation of AI-powered deepfake technology in financial crimes. This fraudulent scheme unfolded in Baotou, a city in Inner Mongolia, where the perpetrator employed AI-

powered face-swapping technology to impersonate a friend of the victim during a video call. Under this false pretence, the fraudster successfully persuaded the victim to transfer a substantial sum of 4.3 million yuan (approximately $622,000), claiming it was needed for a deposit during a bidding process. The victim only realised the deception when the actual friend disavowed any knowledge of the situation, underscoring the escalating risks associated with AI and deepfake technology in criminal activities. As technology continues to blur the lines between reality and deception, addressing personal data protection in an AI-driven landscape becomes paramount.

The contemporary social context, marked by rapid technological progress and a borderless digital universe, mandates the establishment of equivalent and uniform global standards. The digital realm knows no borders, and as such, personal data protection must transcend geographical boundaries. The imperative of creating a harmonised global framework ensures that individuals' rights and privacy remain safeguarded in an increasingly interconnected world.

This thesis does not conclude with a finite answer but opens a doorway to a dynamic and ever-evolving discourse on personal data protection. It reinforces the imperative of vigilance and adaptability in the face of technology's inexorable advance and underscores the profound impact of collective action in shaping the contours of personal data protection for an interconnected world.

In the end, the thesis's culmination is not an ending, but a new beginning, offering a compass to navigate the uncharted waters of personal data protection in an era of boundless technological possibilities.

Bibliography

J.P. Albrecht, *How the GDPR Will Change the World*, European Data Protection Law Review 2, no. 3, 2016.

D. Albrecht, *Chinese first Personal Information Protection Law in contrast to the European GDRP*, Computer Law Review International: A Journal of Information Law and Technology, 2022.

J. Bing, *Transnational Data flows and the Scandinavian Data Protection Legislation*, Scandinavian studies in law 24 1980, October 1980.

F. J. Z. Borgesius, *Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation*, Computer Law & Security Review 32, 2016.

M. Borghi, F. Ferretti, and S. Karapapa, *Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK*, International Journal of Law and Information Technology, Vol. 21, No. 2, 2013.

L. A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, 2002.

L. A. Bygrave, *Privacy and Data Protection in an International Perspective*, Scandinavian Studies in Law, 2010.

L. A. Bygrave, and L. Tosoni, *Article 4(11). Consent In: The EU General Data Protection Regulation (GDPR)*, edited by C. Kuner, L. A. Bygrave, and C. Docksey, Oxford University Press, 2020.

F. H. Cate; P. Cullen; and V. Mayer-Schonberger, *Data Protection Principles for the 21st Century,* books by Maurer Faculty, 2013.

T. Christakis, *Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?*, Randal Milch and Sebastian Benthall (eds), "Cybersecurity and Privacy in a Globalized World - Building Common Approaches", New York University School of Law, e-book (Forthcoming), 14 June 2019.

P. Craig, and G. de Búrca, *EU Law: Text, Cases, and Materials*, 4th Edition, Oxford University Press, 2008.

C. De Terwangne, *Article 16. Right to rectification, in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020.

C. De Terwangne, *Council of Europe convention 108+: A modernized international treaty for the protection of personal data*, Computer Law & Security Review, no. 40, 2021.

P. De Hert and E. Schreuders, *The Relevance of Convention 108*, in European Conference on Data Protection on Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data: present and future, 2001.

E. S. Dove, *The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era*, The Journal of Law, Medicine & Ethics, no. 46, 2018.

D. Erdos, *European Data Protection Regulation, Journalism, and Traditional Publishers*, Oxford University Press, 2019, p.p. 151-152; and S. Gutwirth, Y. Poullet, and P. De Hert, *Data Protection in a Profiled World*, Springer, 2016.

S.Y. Esayas, *The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach*, European Journal of Law and Technology, Vol 6, No 2, 2015.

K. Feng, *Age Criteria of "Children's Consent" in Personal Information Processing (个人信息处理中"儿童同意"的年龄标准)*, Jinan Journal, Philosophy & Social Sciences, No. 8, 2021.

G. Finocchiaro, *Intelligenza Artificiale e protezione dei dati personali*, Giurisprudenza Italiana, July 2019.

L. Floridi, *Pensare l'infospera*, Raffaello Cortina Editore, 2020.

C. Focarelli, *La privacy. Proteggere i dati personali oggi*, Il Mulino, 2015.

A. M. Froomkin, *The Death of Privacy?*, Stanford Law Review, vol. 52, 2000;

F. Gao, *The protection of individuals with regard to processing of personal information-On orientation of "Personal Information Protection Act"*, Academic Monthly (2), 2021.

S. Garfinkel, *Database Nation: The Death of Privacy in the 21st Century*, O'Reilly Media, 2001.

L. Georgieva and C. Kuner, *Article 9. Processing of special categories of personal data in the EU General Data Protection Regulation (GDPR)*, Oxford University Press, 2020.

M. Goddard, *The EU General Data Protection Regulation (GDPR): European regulation that has a global impact*, International Journal of Market Research Vol. 59 Issue 6, 2017.

G. Greenleaf, *Five years of the APEC Privacy Framework: Failure or promise?*, Computer Law & Security Review, no. 25, 2009.

G. Greenleaf, *The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108*, International Data Privacy Law, Volume 2, Issue 2, 2012.

F. Guo, L. Chen, and Y. Jia, 《个人信息保护法》 具体适用中的若干问题探讨 - 基于 《民法典》 与 《个人信息保护法》 关联的视角 (《Gèrén xìnxī bǎohù fǎ》 jùtǐ shìyòng zhōng de ruògān wèntí tàntǎo —jīyú 《mínfǎ diǎn》 yǔ 《gèrén xìnxī bǎohù fǎ》 guānlián de shìjiǎo), 法律适用 (Fǎlǜ shìyòng), No. 1, 2022.

H. Hijmans and C. Raab, *Ethical Dimensions of the GDPR*, *in: Mark Cole and Franziska Boehm, Commentary on the General Data Protection Regulation*, Cheltenham, Edward Elgar, 2018.

W. Huang, *中华人民共和国民法典人格权编解读 (Zhōnghuá rénmín gònghéguó mínfǎ diǎn réngé quán biān jiědú, Interpretation of Personality Rights in the Civil Code of the People's Republic of China)*, China Legal Publishing House, 2020.

K. Ishii, *Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects*, AI & Soc, 2019.

M. L. Jones, *The right to a human in the loop: Political constructions of computer automation and personhood*, Social Studies of Science, Vol. 47, No. 2, 2017.

J. Kokott, and C. Sobotta, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, International Data Privacy Law, Vol. 3, No. 4, 2013.

E. Kosta, *Consent in European Data Protection Law*, Martinus Nijhoff Publishers, 2013.

E. Kosta, *Article 7. Conditions for consent. In: The EU General Data Protection Regulation (GDPR)*, edited by C. Kuner, L. A. Bygrave, and C. Docksey, Oxford University Press, 2020.

W. Kotschy, *Article 6. Lawfulness of processing, in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020.

W. Kotschy, *Art. 83. General conditions for imposing administrative fines, in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020.

H. Kranenborg, *Article 17. Right to erasure ("right to be forgotten"), in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020.

V. Krishnamurthy, *Symposium on the GDPR and International law*, 2020.

D. Krivokapić, and J. Adamović, *Impact of General Data Protection Regulation on Children's Rights in Digital Environment*, Belgrade Law Review, No. 3, 2016.

C. Kuner, *European Data Privacy Law and Online Business*, Oxford University Press, 2003.

C. Kuner, *An international legal framework for data protection: Issues and prospects*, Computer Law & Security Review, 307-217, 2009.

C. Kuner, D. Jerker, B. Svantesson, F. H. Cate, O. Lynskey, C. Millard and N. N. Loideain, *The GDPR as a chance to break down borders, International Data Privacy Law*, 2017, Vol. 7, No. 4, 2017.

C. Kuner, L. A. Bygrave, C. Docksey, *Background and Evolution of the GDPR,* in The EU General Data Protection Regulation: A Commentary, Oxford University Press, 2020.

C. Kuner, *Article 44, General principle for transfer, in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020.

C. Kuner, *Article 49. Derogations for specific situations, in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020.

C. Kuner, *Article 50. International cooperation for the protection of personal data, in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020.

M. Kuschewsky, *The new privacy guidelines of the OECD: what changes for businesses?*, Journal of European Competition Law & Practice, Vol. 5, No. 3, 2014.

S. Kwasny, A. Mantelero, and S. Stalla Bourdillon, *The role of the Council of Europe on the 40th anniversary of Convention 108*, Computer Law & Security Review, no. 40, 2021.

Y. Li, *The Research on the "Dual System" Protection and Claim Basis of the Personal Privacy and Information in The General Principles of Civil Law (论«民法总则»中个人隐私与信息的"二元制"保护及请求权基础)*, Journal of Zhejiang Gongshang University, No. 3 General no. 144, 2017.

E. Lievens, and V. Verdoodt, *Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation*, Computer Law & Security Review, Vol. 34, Issue 2, 2018.

B. Lu, *个人信息保护的"同意"困境及其出路 (Gèrén xìnxī bǎohù de "tóngyì" kùnjìng jí qí chūlù, The "consent" dilemma of personal information protection and its way out)*, Studies in Law and Business, Vol. 38, No. 2, 2021.

M. Macenaite, and E. Kosta, *Consent for processing children's personal data in the EU: following in US footsteps?*, Information & Communications Technology Law, Volume 26, Issue 2, 2017.

H. Mengel, *Internationale Organisationen und transnationaler Datenschutz: Einführung und Dokumentation*, Wissenschaftlicher Autoren-Verlag, 1984.

J. Míšek, *Consent to personal data processing – The Panacea or The dead end?*, Masaryk University Journal of Law and Technology, 2014.

N. Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, Law, Innovation and Technology, Vol 10, No. 1, 40-81, 2018.

R. Queck, A. de Streel, L. Hou, J. Jost, and E. Kosta, *The EU Regulatory Framework Applicable to Electronic Communications*, Telecommunications, Broadcasting and the Internet - EU Competition Law & Regulation, 2010.

M. Ratti, *Personal-Data and Consumer Protection: What Do They Have in Common?,* Studies on Personal Data in Competition, Consumer Protection and Intellectual Property Law, MPI Studies on Intellectual Property and Competition Law 28, Springer Nature, 2018.

C. Ryngaert and M. Taylor, *The GDPR as Global Data Protection Regulation?,* Cambridge University Press, 2020.

L. Scudiero, *Bringing Your Data Everywhere: A Legal Reading of the Right to Portability*, European Data Protection Law Review, Vol. 2, Issue 1, 2017.

A. D. Selbst, and J. Powles, *Meaningful information and the right to explanation*, International Data Privacy Law, Vol. 7, No. 4, 2017.

W. Shen, *On the Construction and Systematization of the Personal Information Right (论个人信息权的构建及其体系化)*, Journal of Comparative Law (比较法研究), No.5, 2021.

T. Streinz, *The Evolution of European Data Law*, in *The Evolution of EU Law*, edited by Paul Craig and Gráinne de Búrca, Oxford University Press, 2021.

C. Sullivan, *EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfer and protection of personal data in the IoT era*, Computer Law & Security Review, no. 35, 2019.

M. Tzanou, *Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right*, International Data Privacy Law, Vol. 3, No. 2, 2013.
H. U. Vrabec, *Data Subject Rights under the GDPR*, Oxford Press, 2021.

P. Voigt, and A. Von Dem Bussche, *The EU General Data Protection Regulation (GDPR) A Pratical Guide*, Springer International Publishing, 2017.

W. G. Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, Business Lawyer, American Bar Association, 2017.

L. Wang, *Legal Protection of Personal Information: Centered on the Line between Personal Information and Privacy (论个人信息权的法律保护-以个人信息权与隐私权的界为中心)*, Modern Law Science, Vol. 35, No. 4, 2013.

C. Wang, *GDPR gèrén shùjù quán yǔ《wǎngluò ānquán fǎ》gèrén xìnxī quán zhī bǐjiào (GDPR 个人数据权与《网络安全法》个人信息权之比较, Comparison of personal data rights under GDPR and personal information rights under the Cybersecurity Law)*, 网络空间张略论坛 Cyberspace Strategy Forum, 2018.

L. Wang, X. Ding, *On the Highlights, Characteristics and Application of Personal Information Protection Law (论《个人信息保护法》的亮点、特色与适用)*, The Jurist, no. 6, 2021.

L. Wang, 论《个人信息保护法》与《民法典》的适用关系 (Lùn "gèrén xìnxī bǎohù fǎ" yǔ "mínfǎ diǎn" de shìyòng guānxì), Huxiang Law Review, no. 1, 2021.

X. Wang, and C. Peng, *Gèrén xìnxī bǎohù fǎlǜ tǐxì de xiànfǎ jīchǔ (个人信息保护法律体系的宪法基础, The Constitutional Basis of the Personal Information Protection Legal System)*, Tsinghua University Law Journal, Vol. 15, No. 3, 2021.

L. Wang, *Mǐngǎn gèrén xìnxī bǎohù de jīběn wèntí -yǐ «mínfǎ diǎn» hé «gèrén xìnxī bǎohù fǎ» de jiěshì wèi bèijǐng (敏感个人信息保护的基本问题-以《民法典》和《个人信息保护法》的解释为背景, Basic Issues of Sensitive Personal Information Protection-With the background of interpretation of «Civil Code» and «Personal Information Protection Law»)*, Dāngdài fǎxué (当代法学, Contemporary Jurisprudence), No. 1, 2022.

L. Wang, Lùn gèrén xìnxī shānchú quán (论个人信息删除权, On the right to delete personal information), Oriental Law (东方法学), No. 1, 2022.

X. Xiao, *Pluralistic Rules on Consent for Personal Information Processing-Analysis and Interpretation based on the Stratum System of Consent (个人信息处理的多元同意规则-基于同意阶层体系的理解和阐释)*, 政治与法律 (Zhèngzhì yǔ fǎlǜ, Politics and Law), No. 4, 2022.

D. Xie, *个人信息跨境提供中的企业合规 (Gèrén xìnxī kuà jìng tígōng zhōng de qǐyè hé guī, On the Corporate Compliance in Cross-border Supply of Personal Information)*, 法学论坛 (Fǎxué lùntán, Legal Forum), 2023.

J. Yao, *System of rights of personal information subjects (个人信息主体的权利体系-基于数字时代个体权利的多维观, Gèrén xìnxī zhǔtǐ de quánlì tǐxì)*, Journal of East China University of Political Science and Law (华东政法大学学报, Huádōng zhèngfǎ dàxué xuébào), No. 2, 2022.

G. Zanfir-Fortuna, *Article 21. Right to object, in: The EU General Data Protection Regulation (GDPR)*, Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press, 2020.

H. Zhou, *个人信息保护的法律定位 (Gèrén xìnxī bǎohù de fǎlǜ dìngwèi)*, Studies in Law and Business, Vol. 37, no. 3, 2020.