FACULTY OF LAW
Lund University

Sandra Wilderoth

EU data transfer requirements for an adequacy decision and the Vietnamese legal realities

JURM02 Graduate Thesis

Graduate Thesis, Master of Laws program
30 higher education credits

Supervisor: Santa Slokenberga

Semester of Graduation: Period 1 Autumn semester 2019

Contents

Summary

In an increasingly globalized world and after the digital revolution, the protection of personal data has fallen in the limelight. Nowadays, data is exchanged over the internet daily for various purposes, including strictly private, commercial, as well as public, which has raised concerns on how these transfers of personal data may affect the right to data protection and the right to privacy.

In the EU context, there has been a tradition to protect personal data, which dates back to 1995, when the Data Protection Directive was adopted. Since then, the data protection within the EU has gradually strengthened, most prominently by the advent of the Charter of Fundamental Rights of the European Union, giving the protection of personal data the formal status of a fundamental right. However, the same trend is not necessarily apparent in countries located outside the EU or other international legal orders apart from the European Council. This leads to the question of how the EU should relate to countries believed providing a lower level of protection of personal data than the level required within the Union?

During the past 20 years, the trade relationship between the EU and Vietnam have become increasingly important. Nowadays, Vietnam is the second-biggest trading partner with the EU among the countries in the Association of Southeast Asian Nations. In June 2019, EU and Vietnam signed a free trade agreement and an investment protection agreement and subject to the European Parliament's approval, some hope they will enter into force within the immediate. While it can be expected that data transfers will increase between the parties, one can question whether there are relevant mechanisms in place to facilitate data exchange and advance the cooperation. In the EU, the most important and comprehensive mechanism for data transfers a so-called adequacy decision. Yet, while Vietnam is ready to be a trade partner,

it might not necessarily be ready for other things that come in parallel with it, as increased data flows.

In this paper, the EU requirements for transferring data to a third country will be examined, focusing on the avenue of an adequacy decision. In parallel, the data protection regime in Vietnam will be scrutinized and tested against the EU standards for adequacy. It will be argued that Vietnam does not meet the EU requirements for adequacy and that the current gap is rather wide, and it is likely to take more than just some amendments in the law to close the gap. Likewise, it will be argued that the EU adequacy requirements are not clear and straightforward, leaving uncertainties to Vietnam and the states in comparable positions.

Sammanfattning

I en allt mer globaliserad värld och efter den digitala revolutionen, har skyddet för personuppgifter hamnat i rampljuset. Numera, utbyts data över nätet dagligen för olika syften, såsom privata, kommersiella och allmänna, vilket har skapat en oro för hur dessa överföringar av personuppgifter kan påverka rätten till dataskydd och rätten till privatliv.

Inom EU har det funnits en tradition av att skydda personuppgifter sedan 1995, när dataskyddsdirektivet antogs. Därefter har dataskyddet inom EU förstärkts, tydligast genom tillkomsten av Europeiska Unionens Stadga om de Grundläggande rättigheterna, som formellt gav skyddet av personuppgifter status som en grundläggande rättighet. Samma trend är inte synlig i länder utanför EU eller i andra internationella rättsordningar, bortsett från Europarådet. Detta aktualiserar frågan om hur EU ska förhålla sig till länder som antas ha en lägre skyddsnivå för personuppgifter än den som krävs inom Unionen?

Under de senaste 20 åren har handelsrelationen mellan EU och Vietnam fått allt större betydelse. Numera är Vietnam den näst största handelspartnern med EU bland medlemsländerna i Association of Southeast Asian Nations. I juni 2019 undertecknade EU och Vietnam ett frihandelsavtal och ett investerings-skyddsavtal och förutsatt att Europeiska Parlamentet ger sitt godkännande finns förhoppningen om att avtalen ska träda ikraft inom kort. Medan dataöverföringar kan förväntas öka mellan parterna, kan det ifrågasättas om relevanta mekanismer finns på plats för att underlätta datautbytet och främja samarbetet.

Inom EU är den viktigaste och mest omfattande mekanismen för dataöverföringar ett så kallat beslut om adekvans. Hursomhelst, även om Vietnam är redo för att vara en handelspartner, är landet inte nödvändigtvis redo för saker som kommer parallellt med det, så som ökade dataflöden.

I denna uppsats kommer EU:s krav för att överföra data till ett tredje land att undersökas, med fokus på ett beslut om adekvans. Parallellt kommer regelverket för dataskydd i Vietnam att granskas och prövas gentemot EU:s standarder för adekvans. Det kommer att argumenteras för att Vietnam inte möter EU:s krav för adekvans, att den nuvarande klyftan är relativt stor och att det troligtvis kommer krävas mer än endast ett par lagändringar för att mötas EU:s krav. Författaren kommer också att visa att EU:s adekvanskrav varken är tydliga eller enkla, utan lämnar en osäkerhet kring vad som gäller för Vietnam och länder i liknande positioner.

Abbreviations

AIS	Authority of Information Security of the Ministry of Information and Communication
ASEAN	Association of Southeast Asian Nations
CJEU	Court of Justice of the European Union
Convention 108	Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data
CSL	Cybersecurity Law
EDPB	European Data Protection Board
EU	European Union
EU Charter	Charter of Fundamental Rights of the European Union
FTA	Free Trade Agreement
GDPR	General Data Protection Regulation
IPA	Investment Protection Agreement
LCIS	Law on Cyberinformation Security
LIT	Law on Information Technology
MIC	Ministry of Information and Communication
PCA	Partnership and Cooperation Agreement
US	United States
WP29	Article 29 Working Party
WP254	Working Paper 254

1 Introduction

1.1 Background

1.1.1 Protection of personal data in the EU

Continued development and expansion of the world trade require that actors in different states can exchange data.[1] In fact, '[i]t has [already] become a truism that data are routinely transferred internationally, and that data processing takes little account of national borders, largely because of the Internet.'[2] For enhanced collaboration, sharing of information is crucial, and in the context of business, it often includes sharing information relating to a person (personal data). At least within the EU, the exchange of personal data triggers the application of the right to privacy as well as the right to data protection.[3] However, when personal data is sent from the Union to another jurisdiction, the protection of these rights might be challenged if they are less protected in the receiving country. [4]

For companies in the EU, the General Regulation on Data Protection (GDPR)[5] is the central framework to comply with when their activities involve the processing of personal data.[6] GDPR sets high standards for the processing of personal data to be lawful, and it lays down both obligations and rights in order to protect the individuals whose personal data is

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ 2016 L 119/1 (GDPR),recital 101.
[2] Christopher Kuner and others, 'The GDPR as a chance to break down borders' (2017) Vol 7, No 4 International Data Privacy Law, 231.
[3] Charter of Fundamental Rights of the European Union [2016] OJ C 202/389 (CFREU), arts 7-8.
[4] Julian Wagner, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) Vol 8, No 4 International Data Privacy Law, 318, 318-319.
[5] See n 1.
[6] GDPR, arts 2 & 3(1).

processed.[7] When a company within the EU wants to send personal data to a recipient in a country outside the Union (a third country or an international organization), whether it is to their branch, another company or public authority, special requirements set out in chapter V of GDPR applies. The purpose is to ensure that the protection of personal data, as guaranteed within the Union, is not undermined by the transfer due to a lower level of data protection in the receiving country.[8]

Under the GDPR, there are three possible avenues for a company to transfer personal data to a third country, lawfully. First, within the scope of an adequacy decision, second, by taking appropriate safeguards or third, by way of derogations in specific situations.[9] An adequacy decision is a decision taken by the European Commission, which states that a particular country, territory or organization ensures an adequate level of protection for personal data. The effect is that personal data can be transferred from the Union to the place in question without any need of specific authorization, as an adequacy decision is binding upon all Member States.[10]

Appropriate safeguards consist of several alternative measures under GDPR, such as binding corporate rules, approved codes of conduct, or standard data protection clauses. Common to all of them, however, is that a supervisory authority must approve the safeguard, either initially or on a case-by-case basis.[11] From a business perspective, therefore, an adequacy decision is preferable, as it causes the least time and cost loss for a company that wants to transfer data to a country outside the EU. Nevertheless, to be subject to an adequacy decision, the third country must be found having a level of data protection that is essentially equivalent to the level guaranteed in the EU.[12]

---

[7] See for example GDPR, arts 5-6, 12-23 and 24-31.
[8] GDPR, arts 3(1) & 44.
[9] GDPR, arts 44-46, 49.
[10] GDPR, art 45.
[11] GDPR, arts 46(2) & 46(3). A closer look at art 46(2) shows that the measures listed nevertheless needs some form of initial approval.
[12] Case 362/14 *Maximillian Schrems v Data Protection Commissioner, Digital Rights Ireland Ltd.* [2015] EU:C:2015:650 (*Schrems* case), para 74 & 96.

1.1.2 EU and Vietnam trade relationship

Since 2015 Vietnam has been the second biggest trade partner with the EU among the countries that are members of the Association of Southeast Asian Nations (ASEAN) and the sixteenth largest trading partner overall.[13] During the past 20 years, Vietnam's Gross Domestic Product (GDP) growth rate has, on average, been around 6 %, and this strong economic development is expected to last in the coming years. Vietnam consists of more than 90 million consumers, a fast-growing middle class, and a young, dynamic workforce.[14] Seemingly, this is a country that has the potential to play a vital role in the world market in the near future and an actor with which a continued good trade relationship could be of great value for the EU.

On the 30 of June 2019, the EU and Vietnam signed a Free Trade Agreement (FTA)[15] and an Investment Protection Agreement (IPA)[16] after starting the negotiations in 2012.[17] Representatives from the EU institutions have described the signing of the EU-Vietnam FTA as 'a milestone.' Further, the former EU Commissioner for Trade, Cecilia Malmström, has described the agreements as 'the most ambitious and comprehensive ones the EU has ever concluded with a middle-income country.'[18] Today the bilateral relationship between the parties is governed by the EU-Vietnam Framework Agreement on Partnership and Cooperation (PCA),[19] which provides Vietnam with trade

[13] Delegation of the European Union to Vietnam, *Guide to the EU-Vietnam Trade and Investment Agreement* (Guide to EU-Vietnam agreements) (Updated in March 2019) <https://eeas.europa.eu/sites/eeas/files/eu_fta_guide_final_3.pdf> accessed 20 November 2019, 7.
[14] Guide to EU-Vietnam agreements, 6.
[15] Commission, 'Proposal for a Council Decision on the conclusion of the Free Trade Agreement between the European Union and the Socialist Republic of Viet Nam' COM (2018) 691 final (FTA).
[16] Commission, 'Proposal for a Council Decision on the conclusion of the Investment Protection Agreement between the European Union and its Member States, of the one part, and the Socialist Republic of Viet Nam, of the other part' COM (2018) 693 final (IPA).
[17] The official website of the European Commission, 'Countries and regions, Vietnam' <https://ec.europa.eu/trade/policy/countries-and-regions/countries/vietnam/> accessed 20 November 2019.
[18] Guide to EU-Vietnam agreements, 6-7.
[19] Framework agreement on comprehensive partnership and cooperation between the European Union and its Member States, of the one part, and, the Socialist Republic of Vietnam, of the other part [2016] OJ L 329/8 (PCA).

preferences towards the EU.[20] However, the new agreements will increase European companies' access to the Vietnamese market and enable them to operate in the Vietnamese postal and banking sectors and to invest in the Vietnamese manufacturing industry. Given that the EU raised its investment stock in Vietnam from 4 to 8 billion euros between the years 2013-2016 and that EU's service export to Vietnam in 2016 amounted to nearly 2 billion euros, the new trade conditions in the FTA and IPA are expected to generate significant economic benefits.[21] Subject to the European Parliament's approval, there are some hopes that the agreements will come into effect in 2020.[22]

1.1.3 A few notes on Vietnam's legal system

A month after the EU-Vietnam FTA and IPA were signed, Asia Law Portal published an article about the personal data protection in ASEAN. It stated that there is 'no indication that Vietnam is moving towards [a] singular data protection law compromising the policies of the EU GDPR.'[23] Slightly earlier, contradictory, Rouse The Magazine claimed that the Ministry of Justice in Vietnam had announced that a decree on personal data protection would be drafted shortly, aiming to create a unified regulation on personal data protection in Vietnam.[24] However, at the moment, Vietnam lacks a horizontal data protection regulation similar to the EU's GDPR, which raises the questions to what level personal data is protected in Vietnam.

---

[20] The official website of the European Commission, 'Countries and regions, Vietnam' <https://ec.europa.eu/trade/policy/countries-and-regions/countries/vietnam/> accessed 20 November 2019.
[21] Ibid, 12-13.
[22] European Parliament, Legislative train 10.2019, 3 International Trade – INTA, *EU-Vietnam free trade agreement (EVFTA)*, p 1 <www.europarl.europa.eu/legislative-train/api/stages/report/10-2019/theme/international-trade-inta/file/eu-vietnam-fta> accessed 7 January 2020.
[23] ASEAN Insiders Series 2019 – Personal Data Protection, see rubric 'ASEAN Data Protection Laws & Readiness for EU GDPR' (19 July 2019) <https://asialawportal.com/2019/07/19/asean-insiders-series-2019-personal-data-protection/> accessed 28 December 2019.
[24] Rouse The Magazine, 'Vietnam: Three new important regulations on data protection in the making' <www.rouse.com/magazine/news/vietnam-three-new-important-regulations-on-data-protection-in-the-making/> accessed 30 December 2019.

Looking at the legal system in Vietnam, it can initially be recalled that the country has undergone significant changes during the last 70 years. After Vietnam declared independence from France in 1954, the country was divided into a northern and a southern part, with different governing powers. Communist North-Vietnam and US-backed South-Vietnam launched an armed conflict which lasted until 1975 when North-Vietnam won the war after US troops had left the country. South-Vietnam was then quickly conquered, and 1976 the country reconciled whereupon the Socialist Republic of Vietnam was founded.[25]

The Vietnamese Constitution,[26] which is the fifth since 1945, provides that the country is a socialist state where the Communist Party of Vietnam is the force leading the society.[27] Further, it states that the Communist Party shall act upon the Marxist-Leninist doctrine and Ho Chi Minh Thought,[28] consolidating that Vietnam's legal system is based on the Soviet legal theory.[29] Accordingly, the law created by the state has long been considered as the only true source of law, and other common sources of law, such as case-law and custom, have been disregarded.[30] However, after the Doi Moi policy (the Renovation policy) was adopted in 1986, changing the country's centrally planned economy to today's socialist-oriented market economy, a partial change in attitude can be seen.[31] Customary law has begun to be recognized in civil transactions, and precedents have received more attention.[32] Despite these more recent changes, Vietnam is often criticized

[25] Utrikespolitiska institutet, Landguiden Vietnam <www.ui.se/landguiden/lander-och-omraden/asien/vietnam/modern-historia/> accessed 17 December 2019.
[26] The Constitution of the Socialist Republic of Vietnam (The National Assembly, 28 November 2013, Hanoi) (Vietnam's Constitution).
[27] Vietnam's Constitution, arts 2(1) & 4(1).
[28] Ho Chi Minh, was one of the founders of the Communist Party of Vietnam, who led the independence movement against France and constituted a key figure in the People's Army of Vietnam during the war between North-Vietnam and the United States, see Utrikespolitiska institutet, Landguiden Vietnam <www.ui.se/landguiden/lander-och-omraden/asien/vietnam/aldre-historia/> accessed 7 January 2020.
[29] Vietnam's Constitution, art 4(1); Mai Hồng Quỳ and others (eds), *Introduction to Vietnamese Law* (Hong Duc Publishing House– Viet Nam Lawyers Association 2015), 25.
[30] Ibid, 28-29.
[31] Ibid, 16-17; Vietnam's Constitution, art 51.
[32] Mai Hồng Quỳ and others (eds), *Introduction to Vietnamese Law* (Hong Duc Publishing House– Viet Nam Lawyers Association 2015), 28-29, 43.

internationally for deficiencies in its legal system, in particular as regards the protection of human rights.[33]

Recently the European Parliament was asked by several non-governmental organizations to postpone its consent to the new EU-Vietnam agreements 'until certain human rights benchmarks are met by the Vietnamese government.'[34] The freedom of expression was said to be curtailed in Vietnam and the judiciary under tight state control, whereat the organizations wanted to see specific actions before the EU-Vietnam agreements entered into force. Inter alia, it was desired that Vietnam ceased monitoring internet usages and that an independent monitoring and complainant mechanism, to address potential human rights impact of the trade agreements by affected individuals, was set up.[35]

The European Parliament itself has, on several occasions, expressed its concerns about Vietnam. In November 2018, the Parliament condemned the abuse of repressive legal provisions restricting fundamental rights and freedoms and urged Vietnam to take both structural and immediate legal actions. The Vietnamese authorities were called on to repeal or amend all repressive laws, for example, a recently adopted Law on Cybersecurity, which according to the Parliament, greatly threatened the right to privacy.[36] The Law on Cybersecurity has been criticized widely on an international level, and the concerns have, for example, related to its demand for data localization and disclosure of customer information upon the Vietnamese authorities' request.[37] With respect to the pending trade agreements between

[33] See n 32, 34, 35.
[34] Joint NGO Call to Postpone Consent to EVFTA and IPA (Brussels, 4 November 2019) <www.icj.org/wp-content/uploads/2019/11/Vietnam-EVFTA-Advocacy-open-letters-2019-ENG.pdf> accessed 30 December 2019.
[35] Ibid.
[36] European Parliament resolution of 15 November 2018 on Vietnam, notably the situation of political prisoners (2018/2925(RSP)).
[37] Giles Cooper and Hau Le 'Vietnam's new Cybersecurity Law: A headache in the making?' (Cecile Park Media, 2018) <www.duanemorris.com/articles/static/cooper_le_cybersecurity_practitioner_0718.pdf> accessed 23 November 2019, 14-15.

the EU and Vietnam, one could argue that it is now imperative to examine the protection of personal data in Vietnam.

1.2 Purposes and research question

In light of the foregoing, the purpose of this paper is to examine the EU data transfer requirements for an adequacy decision and the Vietnamese legal system. More specifically, this paper examines to what extent, if at all, the Vietnamese system is capable of meeting the EU data protection requirements relevant for adequacy and thus has the potential to enhance free movement of personal data between the jurisdictions.

The following research questions will be answered to achieve the objective of this paper. *First*, what are the EU requirements for an adequacy decision? *Second*, whether and to what extent the Vietnamese legal system contains relevant corresponding legal elements (e.g., norms, principles)? *Finally*, what, if any, is the gap between the EU requirements and the Vietnamese legal system in the context of adequacy?

1.3 Method and material

Legal dogmatic, which also can be called doctrinal legal research, is the overall method used throughout this paper. It consists of a systematic, analytic, and evaluative description of the substance of legal norms in a literal sense. Both historical and sociological considerations may be included in this kind of legal exposition, but the essence of legal doctrine is to systemize and interpret valid law.[38] This approach fits very well with the aim of this paper, which is to answer whether Vietnam's data protection regime is adequate from an EU legal perspective and, more specifically, the standard set by the

[38] Aleksander Peczenik 'Legal doctrine and legal theory' in Corrado Roversi (eds), *A Treatise of Legal Philosophy and General Jurisprudence* (Springer, Dordrecht, 2005), para 1(1)(2).

GDPR. Accordingly, a careful examination of the data protection rules both in the EU as well as in Vietnam is required, which the methodology of legal dogmatic enables. Nonetheless, as the matter concerns EU law, particular consideration has also been given to the EU legal method. Thus, the sources of EU law, consisting of the treaties, the Charter of Fundamental Rights of the European Union (the Charter), general principles of EU law and secondary law have been studied with due regard to the case law provided by the Court of Justice of the European Union (CJEU).[39] Finally, it could be noted that the paper applies a comparative perspective in relation to Vietnam, in so far as the data transfer provisions under the GDPR enables it.

In the study of the data protection regime in the EU, GDPR has been the primary source along with case law from the CJEU, working documents from Union bodies and doctrinal writing. Additionally, the other sources of EU law, as presented above, have necessarily been taken into account for the data protection regime in the EU to be presented entirely. It should also be noted that GDPR is, to a large extent, based on the previous Data Protection Directive,[40] whereupon materials referring to the directive also have been used when appropriate.[41] In particular, this applies to the referred case law, and working documents since guidance of this kind relating to the GDPR is still limited due to the regulation young age.[42]

In terms of the peculiarities for data transfers, working documents of the Article 29 Working Party (WP29) has served the most guidance, even though they formally are not legally binding. WP29 was an independent, advisory body created by Article 29 of the Data Protection Directive, with the tasks to provide guidance on the interpretation of the directive and ensure compliance with its provisions.[43] When GDPR became applicable, WP29 was succeeded

[39] See Karl Riesenhuber (ed), *European Legal Methodology* (Ius Communitatis, 1st edn, vol 7, Intersentia, 2017).
[40] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31(Data Protection Directive).
[41] GDPR, recital 9.
[42] GDPR was adopted in April 2016 but became applicable in May 2018, see GDPR, art 99.
[43] Data Protection Directive, arts 29-30.

by the European Data Protection Board (EDPB), who nowadays has the corresponding tasks in relation to GDPR.[44] However, the last two years before WP29 ceased to exist, it began to provide guidance on GDPR, including on data transfer.[45] These working documents were then endorsed by EDPB, but also the older work provided by WP29 remains valid until EDPB states otherwise.[46]

In the study of the data protection regime in Vietnam, legal documents translated into English and published by Thư viện pháp luật (Lawsoft)[47] have been the superior source. As mentioned in the background, Vietnam's legal system is based on a theory in which court decisions are of limited importance and rarely published. As a result, case law on the protection of personal data has not been accessible. Furthermore, the availability of doctrinal writing concerned with data protection in Vietnam has been limited, aware that the language barrier may have been a contributing cause. The additional sources used have, therefore, consisted of a book about the Vietnamese legal system written by Vietnamese scholars and reports from international organizations and law agencies. Finally, to some extent, news articles have been used to alert when information on Vietnam's legal system appears contractionary. However, these latter sources have not impacted on the legal findings made within the limits of this paper.

This paper is part of a Minor Field Study, a scholarship program financed by the Swedish International Development Cooperation Agency, which has enabled the author of this paper to conduct its research in Vietnam.[48] It is hoped that this course of action has led to a better understanding of the legal

[44] GDPR, art 68–70; European Data Protection Board, 'Endorsement of GDPR WP29 Documents' (25 May 2018) <www.edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en> accessed 24 November 2019.
[45] In relation to adequacy decision (art 45 GDPR), see Article 29 Data Protection Working Party, 'Adequacy Referential (updated)' (Adopted on 28 November 2017) (WP254).
[46] GDPR, art 94; European Data Protection Board, 'Endorsement of GDPR WP29 Documents' (25 May 2018) <www.edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en> accessed 24 November 2019.
[47] The accurate translation is 'The Library of Law', however the name used on the English translated site is Lawsoft, <https://thuvienphapluat.vn/> accessed 31 December 2019.
[48] See <www.utbyten.se/program/minor-field-studies/> Accessed 7 January 2020.

system in Vietnam and contributed to more accurate conclusions. Throughout the study, dialogues with both legal professionals working in Vietnam as other Vietnamese inhabitants have been conducted. The purpose of these dialogues has been to identify relevant material and to control the understanding of the sources used, including the accuracy of translations. However, despite these steps, it cannot be ruled out that the referred translated material about Vietnam is inaccurate due to translation service limitations or other reasons, such as political or personal reasons.[49] Finally, it shall be noted that in the context of the legal methods used in this paper, the dialogues have served as information channels only, and the information obtained has had no impact on the legal findings.[50]

1.4 Previous research and delimitations

Data transfers to third countries under the EU data protection regime have been subject to extensive discussion by bodies of the Union as well as of various external actors and scholars.[51] This also applies to the possibility of data transfers in accordance with adequacy decisions, since the European Commission already under the governance of the Data Protection Directive could decide that a third country ensured an adequate level of data protection.[52] However, in relation to Vietnam, data transfers have not been

[49] Due to ethical reasons the author opts for not disclosing any names in the context of this remark.
[50] For the point of clarity, it can be stressed that the analysis of this essay is conducted independently and that the arguments made belongs to the author unless otherwise provided.
[51] Joined cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, Irish Human Rights Commission (intervener), and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others [2014] ECLI:EU:C:2014:238 (Digital Rights Ireland); Article 29 Data Protection Working Party, 'Working Document 01/2016 on the justification on interference with the fundamental right to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)' (Adopted on 13 April 2016) (WP237); Julian Wagner, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) Vol 8, No 4 International Data Privacy Law, 318; Santa Slokenberga and others, 'EU data transfer rules and African legal realities: is data exchange for biobank research realistic?' (2019) Vol 9, No 1 International Data Privacy Law, 30.
[52] See Data Protection Directive, art 25(6); *Schrems* case; WP254.

discussed to any great extent.[53] Moreover, if personal data currently can be transferred to Vietnam without undermining the level of data protection ensured within the EU have not yet been examined. Consequently, it also remains unclear whether Vietnam can meet the EU adequacy standards or, if not, what deficiencies exist in the Vietnam legal system.

This paper seeks to fill the abovementioned gap by examining the adequacy assessment under the GDPR and how the protection of personal data in Vietnam relates to these requirements. However, data transfers based on appropriate safeguards or by way of derogations, which were discussed only briefly in the background to provide a full understanding of the avenues to transfer data under GDPR, have not been further examined.

This study analyses the data protection requirements and has the trade relationship between Vietnam and the EU in its backbone. However, the principles discussed apply equally to data transfers between the EU and other third countries than Vietnam, as well as international organizations in so far as the application of GDPR is triggered. The question on the approval of the FTA and IPA between EU and Vietnam has been highlighted in the background to provide additional nuances to the importance of an adequacy decision in relation to Vietnam. However, more elaborated impacts on trade and data protection, which indeed is an important area of law, have been saved for subsequent studies.

1.5 Structure

This paper consists of four chapters, of which the first one ends after this section. *Chapter 1* has already set the background for the study in terms of

[53] The overall implications of GDPR in Vietnam have drawn attention by some legal practitioners, see, for example Giles Cooper and Hau Le 'Vietnam's new Cybersecurity Law: A headache in the making?' (Cecile Park Media, 2018) <www.duanemorris.com/articles/static/cooper_le_cybersecurity_practitioner_0718.pdf> accessed 23 November 2019, 14-15.

the research question and by highlighting Vietnam's legal realities. *Chapter 2* examines in more detail what GDPR requires to transfer personal data from the EU. Thereafter, *Chapter 3* reviews the adequacy requirements as set forth in Chapter V of GDPR and as elaborated by CJEU and by WP29. In parallel, the Vietnamese legal system is scrutinized to see whether it meets the EU adequacy standards, and central points of identified matches and mismatches between both legal systems, are pinpointed. Finally, *Chapter 4* contains the author's analysis of how Vietnam's legal system currently is corresponding to the EU requirements for adequacy and presents the author's conclusion on how far Vietnam is from having an adequacy decision.

2 Data transfers under GDPR

2.1 Introduction

GDPR aims to ensure a high level of protection of personal data, whether such data flow within the Union or is sent to a third country.[54] To prevent the EU data protection level from being undermined when personal data leaves the Union, a special chapter in GDPR has been devoted to this topic. Chapter V sets out special conditions for transfers of personal data to third countries or international organizations (external transfers), and its provisions apply in addition to all other provisions of GDPR in the event of an external transfer.[55] Article 44 clarifies that not only specific provisions attributable to the specific data transfer must be complied with, but also other requirements from the GDPR shall be observed, in a manner that ensures the level of protection of natural persons as guaranteed within the EU. Thus, in order to lawfully transfer personal data to Vietnam, full compliance with GDPR for the intended processing activity is required, subject to the regulation's material and territorial limitations.

This chapter focuses on unfolding the core requirements stemming from Article 44 in the context of data transfers. It begins with an analysis of key concepts in the processing of personal data and thereby addresses the question of which activities the GDPR applies to. Then, it moves on to analyzing the material and territorial restrictions of GDPR to highlight the limits of its applicability. Finally, this chapter maps out key elements for the processing of personal data that contribute to ensuring the high level of data protection.

[54] GDPR, recital 10, 101.
[55] GDPR, art 44.

2.2 Processing of personal data

2.2.1 Personal data

GDPR applies to 'the processing of personal data,' subject to the exceptions and material and territorial restrictions set forth in section 2.3 of this paper. A key to understanding the applicability of the regulation, therefore, lies in the concepts of *processing* and *personal data*. For the purpose of GDPR, these notions are given a specific meaning in Article 4 and, arguably, a broader one than how they are used in everyday speech.

Personal data refers to any information relating to an identified or identifiable natural person (a data subject).[56] It covers information like names, identification numbers, location data, and online identifiers, but other factors specific to a natural person's identity can also be included. The decisive is whether a person can be identified, directly or indirectly, by reference to the information.[57] However, information relating to deceased persons or legal persons are not considered as personal data under GDPR.[58]

Much information held by businesses in the service industry will qualify as personal data according to GDPR, especially in the tech sector. However, it is worth noting that companies within the manufacturing industry as well will have personal data at their disposal. Aside from the information on their staff, many companies can be assumed to have personal data about their customers or suppliers. For example, a retail company may have its customers' contact details for targeted marketing and their account credentials saved after a sale.

It follows from GDPR's definition of personal data that the information must relate to an identified or identifiable person.[59] This allows for the questioning of whether certain information has reached the threshold for identifiability or

[56] GDPR, art 4(1).
[57] GDPR, art 4(1).
[58] GDPR, recitals 14 & 27.
[59] GDPR, art 4(1).

a sufficient degree of relation.[60] However, from Recital 26 of GDPR, it is clear that the assessment should be comprehensive, and that account should be taken to all means reasonably to be used to identify the natural person. What this could mean, in reality, was clarified by the CJEU in the *Breyer* case.[61]

Breyer case concerned information storage when visiting a website. CJEU stated that all information enabling the identification of an individual does not have to be held by the same person. On the contrary, the court found in this case that a dynamic IP address, registered by an online media service provider, may constitute personal data even when the additional data necessary to identify the individual entering the website, was held by the internet service provider.[62] The decisive was whether the possible means to combine the sources of information was reasonably likely to be used to identify a person. So would not be the case if the measure was prohibited by law or practically impossible due to significant efforts in time, cost, or workforce. However, in the *Breyer* case, CJEU found that 'legal channels' existed since the online media service provider through competent authorities could obtain information from the internet service provider to identify a person in order to bring criminal proceedings, for instance.[63] Accordingly, the threshold for identifiability can be assumed to be set low. This conclusion is also in line with the fact that GDPR, unlike the Data Protection Directive, regards pseudonymized information as personal data since it can be attributed to a person with the use of additional information.[64]

[60] Mike Hintze, 'Viewing the GDPR through a de-identification lens: a tool for compliance, clarification, and consistency' (2018) Vol 8, No 1 International Data Privacy Law, 86, 91-93; Tobias Kugler and Daniel Rücker (eds), *New European General Data Protection Regulation: A Practitioner's Guide* (Bloomsbury Collections 2018) para 68, 72ff.
[61] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] EU:C:2016:779 (*Breyer* case).
[62] Ibid, para 43-44.
[63] Ibid, case, para 45-47.
[64] Pseudonymized data was considered anonymous under Data Protection Directive, see recital 26 compared to GDPR, recital 26.

2.2.2 Processing

Processing is defined by GDPR as 'any operation or set of operation which is performed on personal data or sets of personal data, whether by automated means.'[65] GDPR elaborates this concept by way of giving examples, and a whole range of different activities are regarded as processing such as collection, organization, consultation, dissemination, destruction, and storage. Thus, neither does an operation's intensity and length matter for the qualification as processing nor the required steps for its performance.[66]

GDPR's definition of processing entails that once a company is found to hold personal data, virtually all measures taken regarding such data will constitute processing. To give some examples, all staff management and payroll administration will involve processing when the information concerned is personal data. Similarly, and as for the company's relationship with its customers, sending of promotional emails, storing of IP addresses, and access to contact databases will qualify as processing. To transfer personal data will also constitute processing when the information held is disclosed by the transmission or otherwise made available.[67] However, it must be noted that the qualification as 'processing of personal data' is not sufficient for the application of GDPR in itself. The activity must also fall within the material and territorial scope of GDPR, which will be reviewed in the next section of this paper.

2.3 Material and territorial restrictions

2.3.1 Material scope

GDPR is technology-neutral, and its application does not depend on the equipment used.[68] With that said, Article 2 does restrict the regulation to three

[65] GDPR, art 4(2).
[66] GDPR, art 4(2); Tobias Kugler and Daniel Rücker (eds), *New European General Data Protection Regulation: A Practitioner's Guide* (Bloomsbury Collections 2018), para 51-54.
[67] GDPR, art 4.
[68] GDPR, recital 15.

ways of processing. Firstly, GDPR applies when personal data is processed automatically; secondly, it applies when personal data is processed partly automatically; and thirdly, GDPR applies to manual processing of personal data provided that such data form part of, or will form part of, a filing system.[69] From a business perspective, this means that when personal data is found on companies' computers, smartphones, or other digital aids, GDPR applies.[70] Similarly, GDPR will be relevant if personal data is collected manually but then transferred to smart media for automatic processing, as this constitutes partly automatic processing.[71] This happens when a customer submits their contact information to a cashier in order to receive offers via e-mail, for example. However, if the personal data never will be automatically processed, it must be included in a filing system for GDPR to apply.[72] Article 4 defines a filing system as any structured collection of personal data that is criteria-based, whether centralized, decentralized or dispersed on a functional or geographical basis.[73] Thus, one could argue that invoices containing clients' details, consignments, contracts, and suppliers list in physical forms, probably will be kept sorted in a way that entails the application of GDPR. Photographs on staff or visitors during business events, for instance, will also be covered if kept criteria-based organized.[74]

2.3.2 Controller and processor

In addition to the delimitation to three ways of processing the personal data, GDPR's applicability depends on the people concerned and partly on the location of the processing activity.[75] Jurisdictional issues inevitably impose certain geographical restrictions, although the territorial scope of GDPR has

[69] GDPR, art 2(1).
[70] Storage is a form of processing under GDPR, art 4(2).
[71] David Törngren, Explanatory notes to GDPR 2016, art 2, (Karnov, 1 June 2018) <https://pro-karnovgroup-se.ludwig.lub.lu.se/document/2514469/1> accessed 15 September 2019.
[72] GDPR, art 2(1).
[73] GDPR, art 4(6).
[74] Photographs are personal data when individuals can be identified, directly or indirectly with additional information, see Tobias Kugler and Daniel Rücker (eds), *New European General Data Protection Regulation: A Practitioner's Guide* (Bloomsbury Collections 2018), para 75.
[75] GDPR, art 3.

enlarged the data protection regime as established by the Data Protection Directive.[76] Further, GDPR makes a distinction between two actors, the controller and the processor, as those who can be held responsible for their processing of personal data under the regulation.[77] This distinction was introduced already under the Data Protection Directive.[78]

The *controller* is the actor who determines the purposes and the means for processing personal data while the *processor* is the actor who processes personal data on the controllers' behalf.[79] However, if several actors jointly determine the purposes and means of processing, they will constitute joint controllers, although they individually remain fully liable in relation to the data subject.[80] Processors can also be several in number, but their liability is limited to their respective commitments.[81] Finally, it can be noted that the actors qualifying as controllers or processors can be both natural and legal persons, including public authorities, agencies, or other bodies.

2.3.3 Territorial scope

Article 3 GDPR sets forth three different points of geographical references for the regulations' applicability. The establishment of the actor processing personal data is kept central, but a novelty introduced after the Data Protection Directive, is the effect doctrine.[82] Article 3(2) GDPR states that if an actor established outside the EU processes personal data of subjects within the Union, it must comply with GDPR when the processing relates to the offering of goods or services or the monitoring of the data subjects' behavior.

---

[76] European Data Protection Board, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation' (16 November 2018), 3 <www.edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en> accessed 2 December.
[77] GDPR, art 3.
[78] Data Protection Directive, art 4.
[79] GDPR, art 4(7-8).
[80] GDPR, arts 26, 82(2).
[81] Nevertheless, a processor is liable for its sub-processors, GDPR art 28(1) & 28(4), 82(2).
[82] Tobias Kugler and Daniel Rücker (eds), *New European General Data Protection Regulation: A Practitioner's Guide* (Bloomsbury Collections 2018) para 188.

Thus the effect doctrine, one of the legal bases for extraterritorial jurisdiction recognized in international law, means that the decisive factor is where the action takes effect, not where it is performed.[83] Consequently, GDPR will impose its data protection provisions on actors outside the EU jurisdiction, whenever they choose to process EU subjects' personal data for commercial or monitoring purposes, included in GDPR's material scope.[84]

The main delimitation of GDPR's geographical scope follows from the first point of reference listed in Article 3. It provides that GDPR 'applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.'[85] Hence, the decisive factor is not where the actual processing takes place but that it is performed 'in the context of the activities of an establishment' within the EU. The corresponding criterion existed already in the Data Protection Directive, but its precise content remains unclear.[86] Nevertheless, some clarifications have been made in legal doctrine, case law, and the EDPB guidance.[87]

'In the context of' implies that data processing may take place in one state and be considered as in the context of the activities of an establishment in another state.[88] This is also evident from the wording of Article 3(1) of GDPR. Hence, if personal data is stored by a cloud service provider in Vietnam on a

[83] Wade Estey, 'The Five Bases of Extraterritorial Jurisdiction and the Failure of the Presumption against Extraterritoriality'(1997) Vol 21, No 1, Hastings International and Comparative Law Review, 3, 181, 186.
[84] Benjamin Greze, 'The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives' (2019) Vol 9, No 2 International Data Privacy Law, 109.
[85] GDPR, art 3(1).
[86] Data Protection Directive, art 4(1)(a); Christopher Kuner and others, 'The language of data privacy law (and how it differs from reality)' (2016) Vol 6, No 4 International Data Privacy Law, 259.
[87] European Data Protection Board, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation' (16 November 2018) <www.edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en> accessed 2 December.
[88] Lokke Moerel, 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (2011) Vol 1, No 1 International Data Privacy Law, 28; Tobias Kugler and Daniel Rücker (eds), *New European General Data Protection Regulation: A Practitioner's Guide* (Bloomsbury Collections 2018) para 188.

European company's request, the data must be kept in accordance with GDPR since this constitutes a transfer of data to a third country, whereupon GDPR will apply.

Recital 22 provides some guidance on what is required for a controller or a processor to be considered having 'an establishment' in the EU. It states that effective and real exercise of activity through stable arrangements is needed, but the legal form is not decisive.[89] From case-law, it follows that it is enough that a company has a representative or a bank account in a Member State to be considered established there, and it is not necessary that the company is registered in that state. Finally, it can be noted that 'main establishment' has been explicitly defined in Article 4(16) of GDPR and read together with Recital 36, these provisions may facilitate the interpretation of solely 'an establishment' under GDPR.

2.3.4 Exemptions

From what has been reported so far about the scope of GDPR, there are some exceptions. Somewhat simplified, Article 2 states that GDPR does not apply to process activities outside the scope of EU law, to activities relating to EU's common foreign and security policy, to household activities, or crime prevention measures taken by competent authorities.[90] Sometimes it is ambiguous whether a situation is exempted or not, and Article 2 must be read together with other EU law, not least when it comes to deciding the activities falling outside EU competence.[91]

[89] GDPR, recital 22.
[90] GDPR, art 2(2).
[91] Guidance is also given by the recitals, see recital 16-20 of GDPR.

2.4 Key elements of GDPR

2.4.1 Principles of data processing

GDPR is built around seven principles relating to the processing of personal data, which are set out in Article 5. Additionally, Article 5 contains the principle of accountability, which requires that the controller can demonstrate compliance with the other principles.[92] In the context of data transfers, it follows from Article 44 that it is the company established in the Union that must be able to show that the third country recipient processes the data in accordance with GDPR. It may sound like a task difficult to fulfill but by observing the additional requirements for external transfer as provided for in Chapter V, the company established in EU will demonstrate compliance with the provisions in GDPR.

According to Article 5 GDPR, personal data shall be processed lawfully, fairly and transparent, in relation to the data subject.[93] Arguably, this is particularly important when data are transferred to a third country since the data subject may feel that the transfer entails their data being taken out of their control. The principle of lawfulness is an overarching principle in GDPR, and it takes multiple dimensions. It brings together all GDPR requirements, not only the lawful preconditions of data processing, like the legal basis for the activity under Article 6 GDPR. For instance, the principle permeates Article 9 GDPR, which as a starting point, prohibits the processing of special categories of data (sensitive data, e.g., health data) but also sets conditions that enable lifting the processing ban. Precisely this component is what shields an individual from undesired interferences in the intimate sphere and a legitimate foreclosure from the public.

Transparency is also an overarching obligation under GDPR, and it interlinks both to the data subject's right to be informed as to the controllers'

[92] GDPR, art 5(2).
[93] GDPR, art 5(1)(a).

responsibility to provide the data subject with information.[94] It requires that personal data is collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[95] As regards the latter, limitation of further processing, this will be of specific importance when personal data is transferred. It can be assumed that the data subject wants extra-strong guarantees that their data will not be processed for other purposes than those initially intended when the data is sent to a recipient far away.

The next principles listed in Article 5 provides that kept data should be adequate, relevant, and limited to what is necessary for the processing purpose. Furthermore, the data should be accurate and kept up to date if necessary.[96] With this in mind, the importance of continuous communication between the data subject and the processing companies becomes clear. Regarding data transfers, it is the EU companies' responsibility that both the recipient in the third country and the data subject are sufficiently informed to be able to point out whenever the data undergoing processing needs to be updated.

The last two principles laid down in Article 5 relates to the data subjects' integrity and protection. Firstly, personal data must no longer than necessary for the processing purpose, be kept in a form which permits identification of the data subject. Apart from some exceptions in Article 89, this means that a company involved in processing personal data, do not have the right to preserve the data when the processing purpose has been met.[97] Secondly, personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or otherwise unlawful processing, as well as against accidental loss, destruction, or damage.[98]

[94] Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (As last Revised and Adopted on 11 April 2018) (WP260 rev.01), 4.
[95] GDPR, art 5(1)(b).
[96] GDPR, art 5(1)(c), 5(1)(d).
[97] GDPR, art 5(1)(e).
[98] GDPR, art 5(1)(f).

2.4.2 Data subject's rights

Besides the principles of processing listed in Article 5, GDPR sets out several rights for data subjects as well as several obligations for controllers and processors.[99] Together, these rights and obligations ensure that the principles in Article 5 are realized. Additionally, and as already mentioned, special obligations apply when it comes to data transfers, which will be returned to in Chapter 3.

The rights of data subjects under GDPR include the right to information, the right to access, the right to rectification, the right to erasure, the right to restriction of processing, the right to notification, the right to data portability and the right to object.[100] All of these rights come with their own set of rules, including limitations. Additionally, extensive limitations of data subjects' rights for scientific research purposes or archiving purposes in the public interest, are possible under Article 89 GDPR.

Neither the data subjects' rights, as enshrined in their respective articles, nor the data processing principles in Article 5 are of absolute character. On the contrary, all can be restricted according to the legitimate purposes enumerated in Article 23. However, a restriction must be introduced by a legislative measure, be necessary and proportionate in a democratic society and respect the essence of fundamental rights and freedoms. It can be noted that Article 23 stipulates that the restriction should be provided for by 'Union or Member State law.'[101] One could argue that this statement implies that restrictions of data subjects' rights in third-country legislation cannot be recognized under GDPR. In terms of data transfers, this is of particular importance since it suggests that data transfers to countries where the data subjects' rights are limited cannot take place. However, a contrary interpretation has also been made, namely that the restrictions of data subject's rights listed in Article 23

[99] GDPR, ch 3-4.
[100] GDPR, art 12-22.
[101] GDPR, art 23.

GDPR, also can be acceptable when found in third countries' legislation by an analogous application.[102]

2.4.3 Controller's obligations

A controller's obligations under GDPR are, simply put, to keep records of processing activities,[103] to cooperate with supervisory authorities,[104] to implement appropriate technical and organizational measures,[105]and to conduct a so-called data protection impact assessments or consultation with a supervisory authority if a data subject's rights are exposed to high risk.[106]

The requirement to implement appropriate technical and organizational measures is a new data protection principle introduced by GDPR, referred to as data protection by design and by default.[107] The idea is to avoid infringement of the right to data protection by raising awareness of controllers at an early stage.[108] When deciding measures for data protection by design, the controller should, among other things, consider the state of the art, the implementation costs, and the risk of processing.[109] When it comes to data protection by default, the controller should consider the amount of personal data collected, the storage period, and the data's accessibility.[110]

2.4.4 Oversight and enforcement

In addition to data subjects' rights and controllers' obligations, GDPR set forth requirements for oversight mechanisms and means for enforcement. To ensure compliance with the regulations' provisions, all Member States must

[102] Santa Slokenberga and others, 'EU data transfer rules and African legal realities: is data exchange for biobank research realistic?' (2019) Vol 9, No 1 International Data Privacy Law, 30.
[103] GDPR, art 30.
[104] GDPR, art 31.
[105] GDPR, arts 24-25, 32.
[106] GDPR, art 35-36.
[107] GDPR, art 25.
[108] Tobias Kugler and Daniel Rücker (eds), *New European General Data Protection Regulation: A Practitioner's Guide* (Bloomsbury Collections 2018) para 530.
[109] GDPR, art 25(1).
[110] GDPR, art 25(2).

designate a supervisory authority tasked with monitoring the efficiency of GDPR.[111] The supervisory authorities' importance is also evident from the EU Charter, where they are included as a constituting element of the fundamental right to data protection.[112] A supervisory authority must be acting completely independently, be established by law, and have the competence to carry out investigations, give notifications of alleged infringements, and have the power to issue warnings reprimands.[113] On the EU level, the EDPB is the supreme supervisory body of GDPR, and it is composed of representatives of the Member States' supervisory authorities.[114] Its tasks and functions are similar to the national authorities, but additionally, the EDPB can issue guidelines, recommendations, and best practices concerning GDPR.[115]

An essential function of the supervisory authorities is to receive complaints. Article 77 GDPR provides that data subjects should be entitled to lodge complaints with a supervisory authority. Additionally, the data subjects should have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.[116] The right to an effective judicial remedy also exists against a controller or processor, and in the event of an infringement, the data subject should be compensated for both material and non-material damages.[117] Furthermore, the controller and processor may be subject to administrative fines or other penalties for which the Member State shall lay down provisions.[118]

2.5 Concluding remarks

As this chapter shows, GDPR is triggered when three essential components are met, namely when an activity is regarded as the processing of personal

[111] GDPR, art 51.
[112] CFREU, art 8.
[113] GDPR, arts 52, 54, 58.
[114] GDPR, art 68.
[115] GDPR, art 70.
[116] GDPR, arts 78.
[117] GDPR, arts 79, 82.
[118] GDPR, arts 83-84.

data and not excluded by the regulations material and territorial restrictions. Once a matter falls within the scope of GDPR, not only considerable obligations arise for controllers and processors, but also a set of individual rights for data subjects. Besides, several facilitators to realize the regulation's objective is provided for, such as data processing principles and mechanisms for oversight and enforcement. What precise rights and obligations will be relevant in a particular data transfer situation will depend on the specific case so that a data subject's fundamental right to data protection is not undermined. However, when it comes to data transfers by way of an adequacy decision, there are some key elements to be considered, as now will be accounted for in Chapter 3.

3 Adequacy Requirements and Vietnamese Law

3.1 Introductory remarks

It follows from Article 45(2) of GDPR that an assessment for adequacy shall be comprehensive. The provision lists a number of different elements, divided into three different categories, which the Commission must pay particular attention to. These are a) the data protection regime established through national legislation, b) the existence and effective functioning of independent data protection supervisory authorities and, c) the participation in international conventions or other international commitments giving rise to data protection obligations.[119]

This chapter will examine in depth the requirements that stem from EU law for obtaining an adequacy decision. In parallel, it will scrutinize whether Vietnam's legal system currently corresponds to each of these standards. The structure is as follows. First, the content of an adequacy assessment, as provided for in Article 45(2) of GDPR, will be further elaborated in the light of CJEU's case law and WP29 guidance. Then the data protection principles, as outlined in WP29 guidance on adequacy decisions, working document WP254, will be compared with the content of the Vietnamese legal system. Finally, Vietnam's public authorities' right to access personal data and the country's international commitments on data protection will be reported for.

3.2 Review of adequacy requirements

Article 45(2) of GDPR includes elements which concern a country's entire legal system, such as the respect for the rule of law and human rights and

[119] GDPR, art 45(2); Tobias Kugler and Daniel Rücker (eds), *New European General Data Protection Regulation: A Practitioner's Guide* (Bloomsbury Collections 2018) para 846.

fundamental freedoms. Further, the article states that relevant legislation, of both general and sectoral nature, concerning public and national security, defense, and criminal law, should be reviewed, including public authorities' access to personal data. Naturally, the existence of explicit data protection rules should also be examined, along with professional rules, security measures, and rules for onward data transfers. However, to make a proper evaluation of the legal system in question, the Commission should not merely look for the rules per se, according to Article 45. Likewise, the Commission should consider the rules implementation, relevant case-law, the enforceability of data subjects rights, and finally, the existence of effective administrative and judicial redress for data subjects whose personal data has been transferred.[120]

Although Article 45 of GDPR clearly states what to consider in an adequacy assessment, it is silent on how or to what extent each criterion must be met.[121] However, in this regard, the *Schrems* case[122]and working document WP254 provides some useful guidance.[123] In *Schrems* case, ruled in 2015, CJEU found that the then adequacy decision for the United States was invalid. CJEU held that the Commission had failed to make a proper adequacy assessment by not finding that the United States, *in fact*, ensured an adequate level of data protection by its domestic law or international commitments.[124] The court stressed that even though a third country may resort to other means to protect personal data than those used by the EU, the means must nevertheless prove effective in practice and provide a level of protection *essentially equivalent* to the level upheld in the EU.[125]

As a result of CJEU's statements in the Schrems case and due to the advent of GDPR, WP29 had its previous guidance on adequacy decisions updated.

[120] GDPR, art 45(2)(a).
[121] Julian Wagner, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) Vol 8, No 4 International Data Privacy Law, 318, 319, 322.
[122] See n 12.
[123] WP254.
[124] *Schrems* case, para 97-98.
[125] Ibid, para 74 & 96.

The result was WP254, and it establishes several 'core data protection principles' that must be reflected in a legal system for it to be considered adequate. These principles cover both substantive and procedural aspects, and the purpose of WP254 is to guide the Commission in its assessment on adequacy by concretizing the minimum requirements a legal system must meet to have a data protection level essentially equivalent to the level in EU.[126] In section 3.3.2 and onwards of this paper, the WP254 principles will be reviewed in parallel with an examination of whether these principles are found in Vietnam's legal system. First, however, the respect for the rule of law and human rights in the EU and Vietnam will be scrutinized, as these elements also are included in an adequacy assessment.

3.2.1 The rule of law

3.2.1.1 Content of the rule of law in the EU

The rule of law and respect for human rights are two of the values on which the EU is founded.[127] Besides, the Union shall promote these values, both to its Member States but also in its external relations. Accordingly, respect for these values has been made a prerequisite for an adequacy decision.[128] In terms of the rule of law, it can initially be noted that although the EU treaties explicitly refer to it, CJEU has never exhaustively explained its content.[129] However, over the years, the court has acknowledged certain principles that are inherent in the rule of law, and some have argued that the rule of law is a living instrument, constantly evolving to meet new challenges.[130]

The most prominent principles the CJEU has stated as part of the rule of law include legality, legal certainty, confidence in the stability of a legal situation,

[126] WP254, see introduction and ch 3.
[127] Consolidated version of the Treaty on European Union [2016] OJ C 202/13 (TEU), arts 2 & 6; CFREU, preamble.
[128] GDPR, art 45(2)(a).
[129] Santa Slokenberga, Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal and Tunisia. Adequacy considerations and Convention 108, IDPL pending approval after peer-review (unpublished).
[130] Thomas von Danwitz, 'The Rule of Law in the Recent Jurisprudence of the ECJ' (2014) Vol 37, No 5 Fordham International Law Journal, 1311, 1346.

and proportionality. It also consists of essential procedural principles such as the right to be heard, the right of defense, the right to access the file, and the obligation to properly motivate legal actions.[131] Thus, the core of the rule of law is the judicial review of legislative measures.[132] Additionally, safeguards against the misuse of power are of importance, such as the right to challenge legally binding decisions one is made subject to and the possibility to review the legality of acts adopted by the government.[133]

3.2.1.2 The rule of law in Vietnam

Vietnam's recently very dynamic legal and political history has impacted on how the rule of law now is ensured. Core requirements are set forth in the Vietnamese Constitution, most prominent in Article 2, stating that Vietnam is a socialist state 'ruled by law.'[134] Further, the Constitution expresses the power-sharing doctrine, namely the division of power between the legislative, the executive, and the judiciary, as well as the principle of peoples' equality to law.[135] Thus, the essence of the rule of law seems to underpin the Vietnamese legal system; however, there are contradictions.

A prime example of these contradictions concerns the National Assembly, which has extensive power. According to Vietnam's Constitution, the National Assembly is the highest representative body of the people and the highest state power body in Vietnam.[136] In addition to being the legislature, the National Assembly should conduct supreme oversight of the state activities, including reviewing the activities of the highest judicial body of Vietnam, the Supreme People's Court.[137] The National Assembly both elects

[131] Thomas von Danwitz, 'The Rule of Law in the Recent Jurisprudence of the ECJ' (2014) Vol 37, No 5 Fordham International Law Journal, 1311, 1315-1316.
[132] Joined C 584/10 P, C 593/10 P and C 595/10 P *European Commission and Others v Yassin Abdullah Kadi* [2013] EU:C:2013:518, para 66.
[133] Santa Slokenberga, Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal and Tunisia. Adequacy considerations and Convention 108, IDPL pending approval after peer-review (unpublished).
[134] Vietnam's Constitution, art 2.
[135] Vietnam's Constitution, arts 2 & 16.
[136] Vietnam's Constitution, art 69.
[137] Vietnam's Constitution, arts 69, 70(2), 104.

and relieves the judges from their duty, and it can further suspend the implementation of their source documents.[138] Accordingly, the judiciary power in Vietnam is put in a dependency position to the National Assembly, which is contrary to the rule of law. From CJEU's case law, it follows that effective judicial review is inherent in the rule of law, which requires an independent court-system where the judges can operate without external influence.[139]

Another remark to be made on Vietnam's legal system is that it has been criticized for being legal uncertain and unstable.[140] Many Vietnamese laws prescribe that further details will be provided for by the government, which has allowed the laws to be kept very vague. However, a final date for issuing clarifications is rarely stated whereupon many laws continue to be unspecified and difficult to apply in practice.[141] Additionally, other legal documents, such as Acts and Ordinances, often risk being inconsistent with each other due to the lack of unity and coordination of the Vietnamese legal system. As a result, conflicting provisions are often included in the legal documents, but not infrequently, they say different things.[142]

The Vietnamese Government (the Cabinet) has been tasked with issuing guiding documents to facilitate the laws' applicability.[143] As a matter of division of powers, it is not problematic to delegate competence to issue detailed rules to the executive branch as long as there are relevant principles that steer this delegation. However, the delegation of power between the National Assembly and the Government in Vietnam has been criticized for

[138] Vietnam's Constitution, arts 70(7) & 74(4).
[139] *Schrems* case, para 95.
[140] Mai Hồng Quỳ and others (eds), *Introduction to Vietnamese Law* (Hong Duc Publishing House– Viet Nam Lawyers Association 2015), 32.
[141] See for example, Cybersecurity Law, No. 24/2018/QH14 (CSL) art 12(5).
[142] Mai Hồng Quỳ and others (eds), *Introduction to Vietnamese Law* (Hong Duc Publishing House– Viet Nam Lawyers Association 2015), 32.
[143]Ibid.

being indefinite, leading to an overlap between the legislature and executive.[144]

3.2.2 Respect for human rights and fundamental freedoms

3.2.2.1 Human rights and fundamental freedoms in the EU

The respect for human rights and fundamental freedoms are ensured by EU primary law, in particular by the Charter and the acknowledgment of the European Convention of Human Rights in the EU legal order.[145] Besides, and in addition to what explicitly appears from these two legal acts, the topic of human rights protection in the EU has been subject to extensive academic writing and case law.[146]

The EU Charter provides an overarching right to privacy in Article 7. It also contains rights common in other multinational human rights charters, such as the right to life[147] and the freedom of religion,[148] assembly,[149] and expression.[150] In terms of data protection, the EU Charter, in contrast to many other declarations on human rights, explicitly recognizes a fundamental right of data protection. The right to data protection is found in Article 8 of the EU Charter, which also clarifies what the right in more detail encompasses. Thus, it follows that personal data must be processed fairly, for specified purposes, and on the basis of consent or law. Further, it is stated that everyone should have the right to access and rectify personal data collected about them, and

[144] Mai Hồng Quỳ and others (eds), *Introduction to Vietnamese Law* (Hong Duc Publishing House– Viet Nam Lawyers Association 2015), 32.
[145] See WP254, ch 1; TEU, art.6.
[146] Julian Wagner, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) Vol 8, No 4 International Data Privacy Law, 318, 319, 322.
[147] CFREU, art 2.
[148] Ibid, art 10.
[149] Ibid, art 12.
[150] Ibid, art 11.

that data protection rules shall be subject to control by an independent authority.[151]

3.2.2.2 Human rights and fundamental freedoms in Vietnam

The protection of human rights in Vietnam has gradually expanded and been strengthened in line with the adoption of each new constitution.[152] Nowadays, Vietnam has ratified several important international conventions on human rights such as the International Covenant on Civil and Political Rights, The International Covenant on Economic, Social and Cultural Rights, the Convention on the Rights of the Child, and various conventions of the International Labour Organization.[153] Nevertheless, as mentioned in the background, Vietnam has been criticized by international organizations, including the EU, for disrespecting human rights, such as the right to privacy. Thus, there are two incompatible pictures about Vietnam's legal system, which raises the question of whether the guarantee of human rights only exists in law or whether it also exists in practice.

Article 3 of Vietnam's Constitution states that human and citizens' rights should be recognized, respected, protected, and guaranteed. Further, it follows that restrictions of these rights must be prescribed by law and necessary for reasons of national defense or national security, social order, safety or morality, or for community well-being.[154] Simultaneously, the Constitution provides that the exercise of human and citizens' rights may not infringe on national interest or others' lawful rights and interests.[155] Therefore, the legal position of human rights in Vietnam appears uncertain. It

[151] Ibid, art 8.
[152] Mai Hồng Quỳ and others (eds), *Introduction to Vietnamese Law* (Hong Duc Publishing House– Viet Nam Lawyers Association 2015), 53.
[153] Mai Hồng Quỳ and others (eds), *Introduction to Vietnamese Law* (Hong Duc Publishing House– Viet Nam Lawyers Association 2015), 53-54.
[154] Vietnam's Constitution, art 14.
[155] Ibid, art 15.

can also be worth pointing out that the distinction made between 'human' and 'citizen' rights in the Vietnamese Constitution is in no way further explained.

Several of the fundamental rights protected by the EU Charter has a counterpart in Vietnam's constitution, such as the right to life,[156] the right to freedom of speech[157] and the right to freedom of belief and religion.[158] However, an explicit right to data protection does not exist in the Vietnamese legal system. The right to privacy is recognized in Article 21 of Vietnam's constitution, and it includes 'right to protection of correspondence, telephone conversation, telegrams and other forms of private communication.'[159] Although there are differences between the right to privacy and the right to data protection, it has been argued that, at least partially, personal data is protected by virtue of the right to privacy.[160]

3.3 Substantive requirements

3.3.1 Review of legal requirements of data protection in Vietnam

Vietnam lacks a horizontal law that is only concerned with the protection of personal data. What most closely resembles GDPR within the EU, is the Law on Cyberinformation Security (LCIS);[161] however, its material scope is wider. LCIS provides a general framework for the protection of information and information systems in cyberspace.[162] Thus, LCIS concerns all information appearing in cyberspace, defined as 'an environment where information is

[156] Ibid, art 19; TEU, art 2.
[157] Vietnam's Constitution, art 25; TEU, art 11.
[158] Vietnam's Constitution, art 24; TEU, art 10.
[159] Vietnam's Constitution, art 21.
[160] Juliane Kokott, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) Vol 3, No 4 International Data Privacy Law, 222.
[161] Law on Cyberinformation Security, No. 86/2015/QH13 (LCIS).
[162] LCIS, arts 1 & 3(1).

provided, transmitted, collected, processed, stored, and exchanged over telecommunications networks and computer networks.'[163]

In addition to LCIS, personal data also enjoys some protection through sectoral legislation in Vietnam. For example, the Law on Protection of Consumers' Rights[164] contains several data protection provisions, such as protection of information during collection, use and transfer, an obligation of notification, observance of confidentiality, purpose limitation, right to update and rectification, accountability and right to compensations for damages.[165] Similar provisions can be found in the Law on E-Transactions,[166] the Law on Insurance Business,[167] and the Law on Credit Institutions.[168]

As the material scope of the above mentioned sectoral legislation limits the data protection they provide, the data protection regime in Vietnam becomes fragmented. Consequently, it is difficult to discern any general data protection principles in the Vietnamese legal system, similar to the ones in GDPR. However, in the *Schrems* case, the CJEU clarified that 'a third country legislation does not have to mirror the European data protection regime point by point, but instead has to guarantee the core requirements of the European legislation.'[169] As mentioned initially in this section, WP29 has compiled the EU's core data protection principles in WP254, and as long as these principles are ensured by the Vietnamese laws, Vietnam's data protection regime can still be considered adequate. Therefore, the content of the WP254 principles, and to what extent they are reflected in the Vietnamese laws will be reviewed in the following sections of this paper.

---

[163] Ibid, art 3(1).
[164] Law on Protection of Consumers' Rights, No.59/2010/QH12.
[165] Law on Protection of Consumers' Rights, No.59/2010/QH12, see for example, arts 6-8, 11-13.
[166] Law on E-Transactions, No. 51/2005/QH11, see for example, arts 41-46.
[167] Law on Insurance Business, No. 24/2000/QH10 as amended by Law No. 61/2010/QH12, see for example, arts 19(1), 91(2),124(6) & 125(1).
[168] Law on Credit Institutions, No. 47/2010/QH12, see for example, arts 14 & art 26.
[169] Julian Wagner, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) Vol 8, No 4 International Data Privacy Law, 318, 325; WP254, ch 1.

3.3.2 Data protection concepts

The first principle listed in WP254 can be called 'data protection concepts,' and it provides that 'basic data protection concepts or principles should exist in the third country's legislation. The concepts do not have to mirror the terminology in GDPR, but they should reflect and be consistent with the concepts enshrined in the European data protection law. To illustrate some of the most important concepts found in GDPR, personal data, processing, controller, processor, recipient, and sensitive data are enumerated.[170]

The importance of requiring certain basic data protection concepts in a country's legislation, in order to be subject to an adequacy decision, has been convincingly explained in doctrine. Concepts as personal data and processing in GDPR is decisive for whether and to what extent the regulation applies. Thus, by examining the presence of basic data protection concepts in a foreign legal system, it can be ascertained if the system has a wider or narrower scope than GDPR. This is necessary information to be able to judge whether the third country ensures a level of data protection essentially equivalent to the level in the EU.[171]

Both the concept of personal data and processing are acknowledged and explicitly defined in LCIS. Personal data is called 'personal information' in LCIS, but the meaning is the same, namely 'information associated with the identification of a specific person.'[172] The provision does not address the possibility of indirect identification in contrast to GDPR, nor does it lists examples of different kinds of personal information.[173] However, as the definition reads 'information associated with the identification,' one could

[170] WP254, ch 3(a)(1).
[171] Julian Wagner, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) Vol 8, No 4 International Data Privacy Law, 318, 329-330.
[172] LCIS, art 3(15).
[173] See GDPR, art 4(1).

argue that it is both possible and desirable to adopt an inclusive interpretation to align the provision with the definition in GDPR.[174]

Processing is defined in LCIS as 'the performance of one or some operations of collecting, editing, utilizing, storing, providing, sharing or spreading personal information in cyberspace for commercial purpose.'[175] This implies a discrepancy towards the data protection regime in the EU. Firstly, GDPR includes more activities in the concept of processing, such as erasure and destruction. Secondly, GDPR does not limit the concept of processing to commercial activities.[176] However, if the material scope of GDPR is recalled as previously reported in section 2.3.4 of this paper, the processing of personal data in 'purely household activities' is exempted from GDPR's applicability.[177] Thus, to a certain extent, one could argue that GDPR, like LCIS, is limited to commercial activities.

Counterparts to GDPR's concepts of controllers and processors do not exist in LCIS. Nevertheless, the law applies to Vietnamese agencies, companies (organizations), and individuals, including foreign companies and individuals, whenever they are directly involved in or related to so-called 'cyber information security activities' in Vietnam.[178] Consequently, it appears as GDPR's concepts of controllers and processors are among those actors who can be held liable under LCIS, even though their responsibilities are not divided in the same was as in GDPR.

Finally, it can be noted that GDPR's concepts of recipients and sensitive data does not have any equivalents in LCIS.[179] As was discussed in section 2.4.1 of this paper, GDPR makes a distinction between 'ordinary' personal data and special categories of personal data (sensitive data). Sensitive data may reveal

[174] For a similar conclusion, see Santa Slokenberga and others, 'EU data transfer rules and African legal realities: is data exchange for biobank research realistic?' (2019) Vol 9, No 1 International Data Privacy Law, 30, 41.
[175] LCIS, art 3(17).
[176] GDPR, art 4(2).
[177] GDPR, art 2(c).
[178] LCIS, art 2.
[179] For the definition of recipient, see GDPR art 4(9).

race, ethnicity, political or religious belief, or genetic data, and as a starting point, the processing of sensitive data should be prohibited.[180] Furthermore, GDPR sets additional requirements for the processing of personal data relating to children and personal data relating to criminal convictions.[181] Similar restrictions do not exist in LCIS, but Vietnam's Civil Code contains a right to protection of honor, dignity, and prestige. It follows that everyone has the right to request a court to 'reject' information that adversely affects him or her. If the information is held by mass media, agencies, organizations, or other individuals, they must delete the information upon a court request.[182] Thus, if interpreted broadly, this provision in the Civil Code could provide some protection for sensitive data, including information about criminal convictions. It could also be noted that Vietnam's Criminal Code lays down a possibility to have a criminal conviction expunged, that is, removed as it never occurred.[183] Perhaps, this also can be seen as a measure for protecting personal data relating to criminal convictions.

3.3.3 Data protection principles

The five following principles in WP254, after the data protection concepts, concerns the activity of data processing itself. As will be seen, they are a direct elaboration of the data processing principles found in Article 5 GDPR. The principles are legitimate ground for data processing, purpose limitation, data quality and proportionality, data retention, and at last, security and confidentiality.[184] The first principle of a legitimate ground requires that the basis for the processing activity is lawful, fair, and set out in a sufficiently clear manner. EU acknowledges several grounds as legitimate, for example, provisions laid down by national law, the data subject's consent, the necessity to perform a contract, and the legitimate interest of the controller or a third party unless overruled by the interest of the data subject.[185]

[180] GDPR, art 9.
[181] GDPR, art 8 & 10.
[182] Civil Code, No. 91/2015/QH13, art 34.
[183] Criminal Code, No. 100/2015/QH13, art 69.
[184] WP254, ch 3(a)(1).
[185] WP254, ch 3(A)(2); GDPR, art 5(1)(a) & art 6(1)(a).

In Vietnam's legislation, the principle of legitimate grounds is most clearly expressed in LCIS. From Article 4 and Article 16, it follows that processing of personal information, both within the scope of LCIS as well as for other purposes, must comply with the law.[186] Additionally, LCIS requires that the data subjects' consent is obtained before its personal data is processed.[187] Consent is the only legitimate ground recognized in LCIS for processing personal data, except for state agencies' requests.[188] This is a difference in comparison with GDPR, which recognizes more legitimate grounds for processing personal data, albeit to a data subject's advantage. However, of the wording in LCIS, it appears as the requirement for consent does not apply to state agencies but only to companies (organizations) and individuals. [189] Accordingly, it seems that the Vietnamese state agencies are only limited to process personal data in accordance with the law.

In addition to LCIS, legitimate grounds for the processing of personal data can be found in some of Vietnam's sector laws. For instance, the Law on Information Technology (LIT)[190] provides that personal data may be processed to sign, modify or perform a contract including to calculate charges for the use of products and services in network environments.[191] This seems to correspond to GDPR's recognition of necessary processing for performing a contract.[192] However, regarding LIT, it must be noted that the law seems to overlap the scope of LCIS. LIT applies to 'information technology development'[193] and lays down provisions on the processing of personal information in the 'network environment.'[194] It also applies to the same subjects as LCIS, which makes it unclear what legitimate grounds for data

[186] LCIS, arts 4(1) & 16.
[187] LCIS, art 17(1)(a).
[188] Civil Code, No. 91/2015/QH13, art 38(2) also stipulates that collection, preservation, use and publication of information about someone's private lift requires that persons consent.
[189] LCIS, art 17(1).
[190] Law on Information Technology, No: 67/2006/QH11 (LIT).
[191] LIT, art 21(1).
[192] GDPR, art 6(1)(b).
[193] LIT, art 1.
[194] LIT, arts 21-22.

processing Vietnam recognizes.[195] Still, the validity of LIT may be questioned since it was adopted nine years earlier than LCIS, under another National Assembly and according to Vietnam's previous constitution.

The purpose limitation principle in WP254 entails that personal data must only be processed for specific purposes and not subsequently used in contradiction of those initial purposes.[196] This is also in line with the principle of data retention, requiring that data, in general, must not be kept longer than necessary for the purpose of processing.[197] Further, the principle of data quality and proportionality is closely interlinked with the purpose limitation principle since it requires the data kept to be accurate, relevant, up to date, and not excessive to what is necessary.[198] Returning to Vietnam's legislation, all these principles in WP254 are fully expressed in LCIS, but they do not apply to state agencies.[199] Contradictory, LIT also contains these principles, and an accompanying decree expressly states that the principles also apply to state agencies.[200] As noted above, the legal status of LIT is unclear, but its inconsistency with LCIS makes the legal situation for state actors ambiguous and causes a deficiency according to the rule of law.

The last principle concerned with the data processing activity set out in WP254 is the security and confidentiality principle. It requires security to be observed when personal data is processed, including the use of appropriate technical and organizational measures against accidental loss, destruction, and damage, as well as against unlawful processing. However, when the necessary level of security is decided, state of the art and related costs should be considered.[201]

[195] See LIT, art 2 & LCIS, art 2.
[196] GDPR, arts 5(1)(b); WP254, ch 3(A)(3).
[197] WP254, ch 3(A)(5).
[198] WP254, ch 3(A)(4).
[199] LCIS, arts 17(1)(b), 18(1), 18(2), 18(3).
[200] LIT, art 1 & 21; Decree on Information Technology application in State Agencies' operations, No. 64/2007/ND-CP, art 5.
[201] WP254, ch 3(A)(6).

LCIS provides that agencies, companies (organizations), and individuals must ensure that the personal information they process is protected from unlawful utilization. Further, they must ensure the integrity, confidentiality, and usability of the information they hold.[202] In respect of companies and individuals, there is also an explicit obligation to take appropriate management and technical measures, including complying with standards and technical regulations to protect the information.[203] Once again, however, LIT deviates from LCIS and extends this latter obligation to state agencies.[204] Finally, it can be noted that the security and confidentiality principle also is reflected in Vietnam's Civil Code. The Code lays down some general obligations to keep electronic information on individuals confidential, that inspections of such information must follow by law and that contracting parties with knowledge about each other's private life, must not disclose such information unless otherwise agreed.[205]

3.3.4 Individual rights of data subjects

The lasts principles in WP254 concern the minimum rights of data subjects and the minimum obligations of controllers and processors, which must present in a third country's data protection regime. These are transparency, the right to access, rectification, erasure, and objection, the restriction on onward transfers, and finally, objection to direct marketing and automated decision making.[206] Transparency is, as mentioned in section 2.4.1 of this paper, an overarching obligation under GDPR and a long-established feature of the law of EU.[207] It interlinks with all other data protection principles, and it is an expression of fairness in relation to the fundamental right to data protection.[208]

[202] LCIS, arts 3(1) & 16(2).
[203] LCIS, art 19(1).
[204] LIT, art 21(2)(c); Decree on Information Technology application in State Agencies' operations, No. 64/2007/ND-CP, art 5.
[205] The Civil Code, No. 91/2015/QH13, arts 38(3) & 38(4).
[206] WP254, ch 3.
[207] WP260 rev.01, para 1–2.
[208] Ibid, para 2.

The transparency principle requires that personal data is processed openly and that the data subject is provided with clear, easily accessible, concise, and intelligible information. The information should include the main elements of the processing activity, such as the processing purpose, the controller's identity, and information about the rights of the data subject.[209] However, it follows from Article 23 of GDPR that under certain conditions, for example, to safeguard criminal investigations and national security, the transparency principle can be limited.

Regarding the impact of the transparency principle in Vietnam, there are several shortcomings. LCIS lacks provisions on an information duty, vis-à-vis the data subject during the processing activity, and only requires that consent is obtained before the data collection and that the data subject is notified when its personal data has been deleted.[210] Slightly more detailed, LIT provides that the data subject should be informed about the form, the scope, the place, and the purpose of the use of their personal information.[211] Nevertheless, in comparison with GDPR's requirement on transparency, both laws have clear deficiencies since they neither require that the data subjects are informed about their rights or the controller's identity. It can, however, be noted that the Law on the Protection of Consumers' Rights contains an information obligation in the context of purchases of goods and services. It provides that accurate and complete information about companies and individuals trading with goods and services should be provided, but the provision lacks further specifications.[212]

The principle of the right of access, rectification, erasure, and objection put together the data subject's rights set out in Articles 15 to 19 GDPR. These rights are exercised at the initiative of the data subject, which requires transparency in the data protection regime so that the data subjects know about their rights. The principle entails that data subjects should have the right

[209] WP254, ch 3(A)(7).
[210] LCIS, arts 17(1)(a), 17(1)(c), 18(3).
[211] LIT, art 21(2)(a).
[212] Law on Protection of Consumers' Rights, No.59/2010/QH12, art 8.

to obtain confirmation on whether their personal data is being processed, right to have inaccurate data about them rectified, and right to erasure when the processing is unlawful or no longer necessary.[213]

Returning to Vietnam, all the above-mentioned rights can be found in LCIS and LIT. However, this time, also LIT exempts state agencies, and the rights can only be invoked against individuals and companies.[214] Although, GDPR permits restrictions of these rights under the same conditions as the transparency principle, the complete absence of these rights against Vietnamese state agencies must be seen as a severe shortage.[215] In this context, it can be worth noting that WP254 states that the non-existence of a right to data portability and a right to restriction of processing should not hinder the adoption of an adequacy decision, but the existence of such rights would constitute a plus.[216] Thus, it appears as a data protection regime that lacks these rights must still be able to be considered essentially equivalent to the data protection regime in the EU. However, WP254 is quiet on a possible limitation of the right of access, rectification, erasure, and objection, indicating that these rights must be fully reflected.

The final principles in WP254 are the restriction on onward transfers and the right to object against direct marketing and automated decision making. As to the former, it has been described as a key data protection principle.[217] The importance of limiting onward transfers of personal data can be derived from both Recital 101 of GDPR as well as from the portal paragraph for data transfers in Chapter V, Article 44. The idea is to hinder that the high level of data protection laid down by GDPR is undermined when data is transferred, why also rules restricting onward transfers have been made an explicit

[213] WP254, ch 3(A)(8).
[214] LCIS, arts 18(1), LIT art 22.
[215] WP254, ch 3(A)(8).
[216] WP254, footnote 12; In this context it can be noted that LCIS lay down a right to data portability, art 17(3).
[217] Julian Wagner, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) Vol 8, No 4 International Data Privacy Law, 318, 330.

consideration for adequacy.[218] It follows from WP254 that onward transfers of personal data should only be permitted where the new recipient is subject to rules or contractual obligations, which provides an adequate level of data protection.[219] In doctrine, it has been argued that a third country does not have to restrict onward transfers in the same way as the EU, 'as long as comparable measures against the unhindered flow of personal data are put in place.'[220]

In Vietnam, the Law on the Protection of Consumers' Rights provides that 'consumer information' may only be transferred to third parties upon the consumers' consent or otherwise where provided by law.[221] Further, it follows from LCIS that data subjects can request an individual or a company, who processes their data, to stop providing the data to a third party.[222] In addition to these provisions, there are no conditions in the Vietnamese laws on how personal data may be exported from the country. In comparison with the data protection regime in the EU, it is clear that Vietnam's regulations are not sufficient in this regard.

WP254 provides that data subjects should have the right to object against the processing of their data for direct marketing purposes at any time without charge. In terms of automated individual decision making, including profiling, which significantly or legally affects the data subject, it further follows that such processing must be subject to certain conditions.[223] Regarding Vietnam, both LCIS and LIT are silent on these subjects. However, there is a decree on anti-spamming, which states that advertising emails and messages may only be sent after 'an obvious prior consent' and must be immediately terminated upon a refusal notice from the recipient.[224]

---

[218] GDPR, art 45(2)(a).
[219] WP254, ch 3(A)(9).
[220] Julian Wagner, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) Vol 8, No 4 International Data Privacy Law, 318, 330.
[221] Law on Protection of Consumers' Rights, No.59/2010/QH12, art 6(2).
[222] LCIS, art 18(1).
[223] WP254, ch 3(B)(2).
[224] Decree amending and supplementing a number of articles of the government's decree no. 90/2008/ND-CP dated August 13, 2008 on Anti-spamming (No. 77/2012/NĐ-CP) October 05, 2012, arts 7(1),7(2).

3.4 Procedural requirements and enforcement

3.4.1 EU bar for procedural requirements and enforcement

When the material content of a country's legislation has been examined, the next step in an adequacy assessment is to evaluate the laws' enforceability. If a country's data protection regime is to be real, the effective functioning of its rules is of paramount importance. This is also evident from Article 45 of GDPR, which lists several elements concerning enforcement that must be considered in an assessment for adequacy. These elements include effective and enforceable data subject rights as well as effective administrative and judicial redress for data subjects whose data have been transferred. In addition, the existence of oversight mechanisms in the third country must be investigated and, in particular, the existence of independent supervisory authorities, which is a constitutional right under the EU Charter.[225]

GDPR's requirements for certain enforcement mechanisms and procedural safeguards for an effective data protection regime has also been elaborated by WP29 in their working document WP254. They identified four mechanisms that must exist in a third country's legal system before an adequacy decision, taking into account CJEU's statement in *Schrems* case. Herein CJEU pointed out that although the means to which a third country has recourse for ensuring an adequate level of protection may differ from the means used in the EU, those means must nevertheless prove effective in practice.[226] With this in mind, the following data protection mechanisms were considered as minimum: the existence of at least one competent, independent supervisory authority; a data protection system ensuring a good level of compliance; accountability; and a data protection system providing support and help to

[225] GDPR, art 45(2); EU Charter, art 8.
[226] *Schrems* case, para 74.

data subjects in the exercise of their rights and additionally, appropriate redress mechanisms.[227] To what extent these mechanisms are present in the Vietnamese legal order will be reviewed in the following.

3.4.2 Independent supervisory authority

In WP254, the existence of a supervisory authority competent to supervise data protection rules is identified as necessary for adequacy. Further, it is noted that such authority must have certain features. Firstly, the authority should be tasked with monitoring, ensuring, and enforcing compliance with the country's provisions on data protection and privacy. Secondly, the authority must act completely independently and impartially when performing its duties and neither seek nor accept any instructions. Accordingly, the supervisory authority must have the necessary powers to fulfill its mission and to safeguard the data protection regulation. For instance, the authorities should be able to initiate and conduct their own investigations. Finally, consideration should be given to the authority's budget and staff.[228]

Vietnam lacks a 'pure' data protection authority, which may be explained by the absence of a specific law on data protection. Instead, the Ministry of Information and Communication (MIC), which also is the national regulator of information security, is responsible for supervising the laws in this field.[229] For instance, Article 52 of LCIS provides that MIC should manage the security supervision of information systems nationwide, except where the Ministry of National Defence or the Ministry of Public Security has such competence.[230] Further, it follows that MIC has the responsibility to conduct examinations and inspections under LCIS, as well as handle violations and settle complaints concerning the law.[231] To fulfill its task, MIC has

[227] WP254, ch 3(c).
[228] WP254, ch 3(c)(1).
[229] The Official webpage of the Ministry of Information and Communication of the Socialist Republic of Vietnam, 'Main functions' <http://english.mic.gov.vn/Pages/ThongTin/114253/Main-Functions.html> accessed 23 December 2019.
[230] LCIS, art 52(2)(c).
[231] LCIS, art 52(2)(h).

established the Authority of Information Security of the Ministry of Information and Communication (AIS). Subject to MIC's instructions, AIS is responsible for supervising compliance with information security regulations, analyzing and publishing reports on the status of the information security in Vietnam, and receive complaints concerning violations of information security regulations.[232]

In comparison with the guidance in WP254 and Chapter VI GDPR on 'Independent supervisory authorities,' it seems clear that the Vietnamese data protection regime is flawed in terms of the requirement for independence. AIS can only act within the framework of MIC's instructions, and MIC itself is both responsible for elaborating regulation in the field of information security and for supervising the compliance with these laws.[233] The division of power between the legislature, the executive, and the judicial, which is inherent in the rule of law and an element required in a foreign country's data protection regime, therefore appears to be ignored in some areas in the Vietnamese legal system.

3.4.3 Level of compliance and accountability

Mechanisms ensuring a high level of compliance with the third country's data protection regime is the next procedural requirement for adequacy in WP254. In this regard, effective and dissuasive sanctions are mentioned as methods which can play an important role. Verification systems by authorities, auditors, or independent data protection officials are also enumerated, which interlinks with the demand for accountability.[234] As previously mentioned in section 2.4.1 of this paper, accountability is among the principles listed in Article 5 of GDPR, and it refers to controllers' responsibility to demonstrate compliance with the regulation. Therefore, WP29 has found that a corresponding responsibility should exist in a third country's data protection

[232] Data Protection in Vietnam: Overview, see rubric 'Enforcement and sanction', Question 25 <www.amchamvietnam.com/wp-content/uploads/2019/05/Data-Protection-in-Vietnam-Overview-April-2019.pdf> accessed 24 December 2019.
[233] LCIS, art 52(2)(a).
[234] WP254, ch 3(c)(2).

regime. WP254 provides examples of ways for a data protection regime to ensure the principle of accountability, and these include keeping records or log files of data processing activities during a reasonable time, conducting data protection impact assessments, taking data protection by design and by default and designating a data protection officer.[235]

In Vietnam, both individuals and companies are under obligation to take appropriate organizational and technical measures to protect the personal information they hold, according to LCIS and LIT. Article 16 LCIS also provides that individuals and companies (organizations) shall develop and publicize their protecting measures, which suggests a form of accountability. In terms of keeping records, this is not an explicit requirement of either LCIS or LIT. In the former, state agencies have a general obligation to 'secure and store the personal information they have collected.'[236] However, it is not clear if and in such case how, this responsibility can be accounted for. In addition, Article 15 of LCIS lays down a general obligation for agencies, organizations, and individuals to coordinate with competent state agencies in ensuring cyberinformation security, which could be considered as a form of accountability towards state agencies. However, more clearly, LIT provides that companies and individuals should submit to management, inspection, and examination by competent state agencies and meet those agencies' requirements on ensuring information infrastructure safety and information security.[237]

WP254 identifies effective and dissuasive sanctions as one possible way of ensuring high compliance with data protection rules. Regarding the legal system in Vietnam, it can be noted that infringement of laws is generally sanctioned with both administrative and criminal penalties, including compensation for damages. That is also the case in LCIS and LIT.[238] The actual punishment follows from the Criminal Code and, for the illegal

[235] WP254, ch 3(c)(3).
[236] LCIS, art 17(2).
[237] LIT, art 60(2).
[238] LCIS, art 8; LIT, art 77.

provision or use of information on computer networks or telecommunication networks, an administrative fine between 30 million to 1000 million Vietnamese Dong (VND) can be imposed depending on the actual act and its severity.[239] One million VND corresponds to approximately 39 euro, whereupon the fines may be between 1170 to 39 000 euro. Alternatively, an offender may be sentenced to imprisonment between three months and seven years, or in some cases, the punishment may be up to three years of community sentence.[240]

In doctrine, it has been noted that GDPR, in comparison with the old data protection regime in the EU, has extended and improved the procedural and enforcement mechanisms for data protection.[241] Not least, this applies to the administrative fines set out in Article 83 of GDPR, which nowadays can amount to 20 million euros or 4 % of the worldwide annual turnover of the infringer. The increased fines in GDPR have been said to be one of the most important improvements since the Data Protection Directive, which leads to the question of whether a foreign data protection regime must have equally stringent fines to provide an adequate level of data protection. To support that so is the case, GDPR's recitals have been highlighted, which states that the new enforcement and procedural mechanisms in GDPR aim to strengthen the data protection in the EU.[242] However, if a country with less severe sanctions for data protection infringements could be subject to an adequacy decision and thus, receive personal data without further safeguards, the protection provided by GDPR would quickly be undermined. It has therefore been argued that the sufficiency of the enforcement and procedural mechanisms in

[239] Criminal Code, No. 100/2015/QH13, art 288(1)(a), 288(1)(b), 288(1)(c) & 291.
[240] Ibid, art 288(1)(a), 288(1)(b), 288(1)(c). It can be noted that less severe penalties for infringements of Vietnam's data protection rules have been suggested by legal practitioners but without any reference to a legal provision, see for example Data protected Vietnam, see rubric 'Practice' <www.linklaters.com/en/insights/data-protected/data-protected---vietnam> accessed 24 December 2019.
[241] Julian Wagner, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) Vol 8, No 4 International Data Privacy Law, 318, 335.
[242] GDPR, recitals 129 & 148; Julian Wagner, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) Vol 8, No 4 International Data Privacy Law, 318, 335.

a third country must be assessed from a strict EU point of view. At the same time, it has been said that the 'exact amount of the threatened fine by the GDPR may only be a first clue to the minimum protection standard that a country's data protection regime has to provide in order to be deemed adequate.'[243]

3.4.4 Redress mechanism

The last procedural mechanism identified in WP254 focuses on data subjects' actual opportunities to exercise their rights in the third country. The country's data protection regime must provide legal remedies and support to individuals, so that regulatory compliance can be ensured rapidly, effectively, and without prohibitive cost. WP254 claims that this requires a supervision mechanism that allows for investigations of complaints and identification as well as punishment of any violation of data subjects' rights. Whenever it is shown that the data protection rules are not complied with, the data subject should be provided with effective administrative and judicial redress, including compensation for damages caused by the unlawful action. It is said that a redress mechanism is 'a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions to be imposed when appropriate.'[244]

In Vietnam, the clearest provisions on redress mechanisms for data protection infringements follows from LCIS and LIT. Article 20 of LCIS provides that state agencies are responsible for establishing online information channels for receiving petitions and reports from the public related to security assurance. Arguably, this provision aims to facilitate the process for individuals to exercise their rights in case of a data protection infringement. Further, Article 13 LCIS states that incidents of cyber information security should be handled and remedied prompt, accurate, and effective.[245] Beyond these provisions,

[243] Julian Wagner, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) Vol 8, No 4 International Data Privacy Law, 318, 336.
[244] WP254, ch 3(c)(4).
[245] LCIS, art 13(2)(a).

LCIS only states that MIC is responsible for coordinating the response to cyberinformation security incidents nationwide and should prescribe further details for this coordination.[246] In terms of LIT, it contains a provision on the settlement of disputes on technology information, which includes disputes on the exchange of personal information. It provides that settlement through conciliation is encouraged, but alternatively, disputes should be settled in accordance with the law.[247]

In practice, it has been argued that laws on privacy are not legally enforced in Vietnam. The law firm Linklaters published in 2017 a compilation of the data protection in Vietnam, wherein it was claimed that there have been 'some cases' of imposing administrative fines for breaches of personal privacy in Vietnam. It was further said that exact statistics on enforcement actions are missing since the majority are not published, but that leaking of personal data is a common situation in Vietnam, particularly phone numbers to service providers.[248] A non-practice of effective enforcement of data protection rules in Vietnam has also been claimed by the legal publishing company Practical law, as late as in 2019.[249]

3.5 Public agencies access to data

The working document WP254 contains a separate chapter on data protection guarantees in the light of law enforcement and national security measures in third countries.[250] Not infrequently, these kinds of activities will involve the processing of personal data, and although the purpose may be legitimate, it does not justify unlimited access and use of personal data. In the field of surveillance, WP29 has previously provided guidance on what can be

[246] LCIS, art 13(4).
[247] LIT, art 4 & art 75.
[248] Data protected Vietnam, see rubric 'Practice' <www.linklaters.com/en/insights/data-protected/data-protected---vietnam> accessed 24 December 2019.
[249] Data Protection in Vietnam: Overview, see rubric 'Enforcement and sanction', Question 25 <www.amchamvietnam.com/wp-content/uploads/2019/05/Data-Protection-in-Vietnam-Overview-April-2019.pdf> accessed 24 December 2019.
[250] WP254, ch 4.

regarded as justifiable interferences to fundamental rights by state authorities in a democratic society.[251] However, essential guarantees for limiting public authorities' infringements of the right to protection of personal data and the right to privacy must also exist in the field of law enforcement and national security. Therefore, WP254 finds the following guarantees as essential for a data protection regime to be considered adequate: 1) legal basis for the processing; 2) necessity and proportionality with regard to the legitimate objectives pursued; 3) independent oversight of the processing and; 4) availability of effective remedies.[252]

In terms of public authorities' access to personal data, the ongoing *Schrems II* case[253] is of interest. In *Schrems II*, CJEU has been asked to clarify whether EU law applies when personal data is transferred to a third country for commercial purposes but may be further processed by the receiving country's public authorities for national security purposes.[254] The question is based on the material scope of GDPR, which excludes activities for the purpose of public security.[255] At the moment, CJEU has not delivered its judgment, but according to the Advocate General's opinion, EU law applies since a data transfer 'as such' constitutes processing. In the opinion, it was said that as long as the purpose of the data transfer was commercial, any potential subsequent processing is irrelevant. However, if the initial purpose of the transfer had been to give the authorities in the third country access to the data for national security purposes, GDPR would not have been applicable.[256]

[251] WP237, ch 1.
[252] WP254, ch 4.
[253] Case 311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian *Schrems* with others [2019] EU:C:2019:1145, Opinion of AG Saugmandsgaard Øe (*Schrems II* case).
[254] Case 311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian *Schrems* with others [2019] EU:C:2019:1145, Opinion of AG Saugmandsgaard Øe, para 76.
[255] The question was submitted to CJEU under the governance of Data Protection Directive, which exempted processing of personal data for public security from its scope by Article 3(2). The same has continued to apply under GDPR, by virtue of Article 2(2)(a) and Article 2(2)(d) reflecting the Union's allocation of competence stated in Article 4(2) TEU; See Case 311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian *Schrems* with others [2019] EU:C:2019:1145, Opinion of AG Saugmandsgaard Øe, para 102.
[256] Ibid, para 104-106.

In support of its opinion in the *Schrems II* case, the Advocate General referred to Article 45(2) of GDPR. From this provision, it follows that the European Commission should consider the public authorities' access to personal data in its assessment for adequacy, whereupon the possibility of foreign authorities' processing of personal data, can not render GDPR inapplicable to the data transfer itself.[257]

When considering Vietnam's legal safeguards against indiscriminate data processing by its public authorities, some foundings in the previous sections of this paper must be recalled. Firstly, Vietnam's Constitution provides that infringement of human rights for reasons of national security must be necessary and follow by law, although it also states that the exercise of human rights may not infringe on national interest.[258] Secondly, the shortcomings of the independent oversight and the effective remedies in the Vietnamese data protection regime affects the country's legal safeguards against unjustified data processing by its authorities.[259]

LCIS and LIT lack provisions specifically concerned with national security, but both laws permit Vietnamese state agencies to access personal data.[260] For example, Article 17 LCIS provides that a request by a competent state agency legitimizes that a company or an individual discloses personal data to them. However, in terms of national security, the recently adopted Cybersecurity Law (CSL)[261] is of primary interest. The law regulates activities to protect national security in cyberspace, and it appears as it gives the Vietnamese authorities a far-reaching right to access personal data.[262]

---

[257] GDPR, art 45(2)(a); Case 311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian *Schrems* with others [2019] EU:C:2019:1145, Opinion of AG Saugmandsgaard Øe, para 108.
[258] See section 3.2.2.2 in this paper; Vietnam's Constitution, art 14-15.
[259] See section 3.4.2 and 3.4.4 in this paper.
[260] See for instance LCIS, art 20(2) which provides that state agencies shall, annually or when necessary, inspect and examine personal information-processing organizations and individuals which can be assumed to involve access to personal data; LIT, arts 18(3)(a), 20(1), 20(2).
[261] See n 141.
[262] CSL, art 1.

CSL prohibits many different kinds of activities, classified as threats against national security.[263] For example, social evils, destruction of fine traditions, and insult of great men are listed as criminalized behaviors, but since they are based on subjective values, their objective content becomes uncertain. What actions are considered to threaten national security will depend on the moral and cultural values prevailing at the time of assessment, which makes the legal situation uncertain. Accordingly, CSL does not meet the requirement of legal security that follows from the rule of law.[264]

To what extent the public authorities in Vietnam can access personal data under CSL cannot be answered with certainty. Article 5 of CSL lists the measures available to protect national security, and among other things, it entitles the authorities to evaluate, inspect, and supervise the cybersecurity. What this means in more concrete terms, is partly stated in the subsequent articles.[265] For instance, Article 13 CSL defines the concept of inspections, namely as 'the activity of identifying the actual cybersecurity status of the information system and of its infrastructure or of information stored, processed and transmitted on it.'[266] With supervision is meant the activity of collecting and analyzing the current status of an information system, in order to identify cybersecurity threats and incidents, any weaknesses or security vulnerabilities, or malicious codes and hardware.[267]

Article 26 of CSL provides that companies providing services on telecom networks and the internet must provide user information to the Cybersecurity Task Force under the Ministry of Public Security when so requested. The information should be provided in writing, and the purpose is to serve investigation of and dealing with breaches of CSL.'[268] However, more details on what the request should be based on or a requirement on a certain degree

[263] CSL, art 8.
[264] Thomas von Danwitz, 'The Rule of Law in the Recent Jurisprudence of the ECJ' (2014) Vol 37, No 5 Fordham International Law Journal, 1311.
[265] See e.g., CSL, arts 11-15.
[266] CSL, art 13(1).
[267] Ibid, art 14(1).
[268] Ibid, art 26(2)(a).

of suspicion does not appear. Thus, the lack of specifications in CSL entails that the law does not provide the essential guarantees identified as necessary in WP254. The law does not provide a clear and predictable legal basis for legitimizing the Vietnamese authorities' access to personal data, albeit the authorities' powers under CSL are difficult to determine in the absence of an implementing decree.[269] Finally, it can be noted that the reason why CJEU repealed the adequacy decision for the US in the first *Schrems* case, was because it was not shown that the US had adopted rules to limit its authorities' access to personal data.[270]

3.6 International commitments

The last element listed in Article 45 GDPR, to be considered by the Commission in an assessment for adequacy, is whether the third country is a party to any international convention or other legally binding instrument giving rise to data protection requirements. For instance, data protection obligations could follow from the participation in a multilateral or regional system.[271] In this regard, accession to Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108) and its additional protocol must be taken into account according to Recital 105 GDPR.[272] Convention 108 is an international treaty that any country can sign, and thereby the country agrees to secure the right to privacy by implementing appropriate rules in its legal system.[273] All Member States, including the EU itself, are party to Convention 108 but very

[269] Cooper G and Le H, 'Vietnam's new Cybersecurity Law: A headache in the making?' (Cecile Park Media, 2018) <www.duanemorris.com/articles/static/cooper_le_cybersecurity_practitioner_0718.pdf> accessed 23 November 2019, 14-15.
[270] *Schrems* Case, para 88, 98.
[271] GDPR, art 45(2)(c).
[272] The Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108).
[273] Julian Wagner, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) Vol 8, No 4 International Data Privacy Law, 318, 326.

few non-European counties have currently signed the convention, and Vietnam is not one of them.[274]

At present, Vietnam has made a few international commitments with relevance for data protection, although both LCIS and LIT envisages international cooperation in the field of cyberinformation security and information technology.[275] However, Vietnam is a party to the International Covenant on Civil and Political Rights, which prohibits arbitrary or unlawful interference with persons' privacy and correspondence. Although this prohibition lacks details, one could argue that it at least partly provides a right to data protection.[276] A similar provision can also found in the Universal Declaration of Human Rights, but the declaration is not legally binding.[277]

In terms of the international treaties mentioned above, none of them provides effective remedies for data subjects in case of data protection infringements. However, as mentioned in the background, Vietnam is a member of ASEAN, and this association adopted a general framework on data protection in 2012.[278] According to the framework, it aims to strengthen the protection of personal data in ASEAN and to facilitate cooperation between the member states as well as with other countries. Nevertheless, the framework states that it only serves as a record of the ASEAN members' intentions and does not provide any legally binding obligations.[279]

---

[274] The official website of the Council of Europe, 'Charts of signatures and ratifications of Treaty 108' <www.coe.int/en/web/conventions/full-list//conventions/treaty/108/signatures?p_auth=g1E83e21> accessed 27 December 2019.
[275] LCIS, arts 6, 51(11), 52(2)(g), 52(4)(g); LIT art 6(5), 25(2)(d), 65, 66.
[276] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, 171 & 275.
[277] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).
[278] ASEAN Telecommunications and information technology ministers meeting (Telmin), 'Framework on personal data protection' <https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf> accessed 28 December 2019.
[279]Ibid, art 2 <https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf> accessed 28 December 2019.

In terms of the trade relationship with the EU, Vietnam has made certain commitments about its data protection. Currently, the trade relationship between the EU and Vietnam is governed by the PCA, which entered into force 2016.[280] PCA was adopted to strengthen the overall bilateral relationship between the EU and Vietnam, and it contains provisions on cooperation in various areas, such as human rights, the rule of law, and data protection.[281] However, Article 26 on data protection constitutes mostly a position. It reads '[t]he Parties agree to cooperate in order to improve the level of protection of personal data to the highest international standards, as appropriate, such as those contained in international instruments, in so far as they apply to the Parties.'[282] Thus, it follows that neither any concrete obligations or rights in relation to controllers, processors, or data subjects can be derived from the PCA.

Of greater interest, arguably, is whether the EU-Vietnam FTA and IPA contain any provisions on data protection. Although these agreements are not yet in force, they have been signed and obtained their final form.[283] The FTA contains one article, Article 8.45, which explicitly addresses the processing of personal data. It provides that 'each party shall adopt or maintain appropriate safeguards to protect personal data and privacy, including individual records and accounts.'[284] The second paragraph concerns data transfers and it reads that '[n]o later than two years from the date of entry into force of this Agreement, each Party shall permit financial service suppliers of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service suppliers.'[285]

---

[280] The official website of the European Commission, 'Countries and regions, Vietnam' <https://ec.europa.eu/trade/policy/countries-and-regions/countries/vietnam/> Accessed 20 November 2019.
[281] PCA, art 2(d), 2(f).
[282] PCA, art 26(1).
[283] European Parliament, Legislative train 10.2019, 3 International Trade – INTA, EU-Vietnam free trade agreement (EVFTA) <www.europarl.europa.eu/legislative-train/api/stages/report/10-2019/theme/international-trade-inta/file/eu-vietnam-fta> accessed 7 January 2020.
[284] FTA, art 8.45(1).
[285] FTA, art 8.45(2).

Since Article 8.45 of the EU-Vietnam FTA envisages transfers of personal data, at least between financial service suppliers, it may be asked why the agreement lacks more concrete data protection commitments. In several provisions, the FTA states that neither party is prevented from protecting personal data and privacy, as long as the measures adopted are not inconsistent or circumvents the agreement.[286] The requirements for data protection thus appear to a large extent have been left to be decided by the respective party. From a trade perspective, it can be questioned whether this approach is favorable.

In customs matters, the to the FTA associated protocol no. 2 on mutual administrative assistance, provides that personal data may only be exchanged where the receiving party undertakes to protect such data in a manner that is considered adequate by the sending party.[287] However, as the name of the protocol reveals, its provisions are limited to customs matters. Finally, it can be noted that the IPA also contains one provision that addresses data protection. It provides that measures for the protection of personal data, which are necessary to secure compliance with laws or regulations of one party's legal system, can be adopted and enforced, as long as such measures are compatible with the IPA.[288]

3.7 Concluding remarks

The EU sets rather high adequacy requirements, although parts of them are difficult to define thoroughly. The elements for adequacy in Article 45 GDPR does not specify how the assessment should be made in practice, and this affects how precisely the adequacy level can be assessed in a third country in the absence of further details. As scholars rightly have criticized the European Commission for, it has not released full guidance on the adequacy assessment,

[286] FTA, art 8.45(3), 8.53(e)(ii), 12.47.
[287] FTA, protocol n 2, art 10.
[288] IPA, art 4.6(e)(ii).

which casts doubt of transparency about the methodology.[289] What concerns the Vietnamese legal system, obvious differences emerge with the EU legal standards. Nonetheless, the extent to which these differences are hurdles to reaching adequacy and thus an obstacle for free movement of personal data between the EU and Vietnam remains to be discussed in the final chapter of this paper.

[289] Alex Boniface Makulilo, 'Data Protection Regimes in Africa: Too Far from the European "Adequacy" Standard?' (2013) 3 International Data Privacy Law 42.

4 Adequacy requirements and Vietnamese law: miles apart?

4.1 Central reflections as points of departure

The overarching aim of this paper was to examine to what extent, if at all, the Vietnamese system is capable of meeting the EU data protection requirements for adequacy, and thus whether Vietnam has the potential to enhance free movement of personal data between the jurisdictions. In that regard, essential requirements of the GDPR were analyzed, including the adequacy requirements as well as the data protection regime in Vietnam. What now is left, is to address the nucleus of the aim and scrutinize what, if any, is the gap between the EU requirements and the Vietnamese legal system in the context of adequacy?

Already by first glance, it can quickly be ascertained that the data protection regime in the EU is extensive. The 173 recitals and 99 articles of GDPR draws attention; however, its material and territorial scope are the most conspicuous. Besides the comprehensive definition of the key concepts of personal data and processing, the data protection rules in GDPR are neutral to the kind of technology used, the data subject's citizenship, and the place of action. In an increasingly interacting world, where national borders have become invisible through the advent of the internet, the EU may have felt that a wide-ranging data protection regime was both desirable and necessary. Still, however, the far-reaching approach of GDPR is unique from a global perspective.

Currently, the status of data protection as a fundamental right is only emerging in the national legal orders outside the EU. One could argue that the EU tries to speed up this process by adopting GDPR with extra-territorial

obligations and special requirements for data transfers, and aims to lay down the path for a global standard.[290] Whether this will succeed only time can tell, but it may be questioned who bears the risk of failure, the EU, the European companies, or the data subjects?

To date, the EU has shown no signs of wanting to reduce trade and cooperation with third countries where the protection of personal data seems weak. The negotiations of the EU-Vietnam agreements clearly show this. Both the FTA and the IPA lack effective commitments in terms of data protection, even though the EU itself has criticized Vietnam for disrespecting fundamental rights, including the right to privacy. Moreover, the FTA explicitly envisages data transfers between financial service suppliers in the EU and Vietnam, and GDPR explicitly states that continued development of trade requires data transfers. However, when data is transferred to a third country that is not subject to an adequacy decision, it is the European companies who are responsible for taking appropriate safeguards to ensure that the EU level of data protection is maintained after the transfer. If they fail, high fines wait to be paid according to the standards set forth in Article 83 of GDPR.

4.2 Vietnam's proximity to adequacy

4.2.1 Substantive deficiencies

When the requirements for adequacy have been elaborated vis-à-vis the data protection rules in Vietnam (see chapter 3), discrepancies have been made visible in several respects. None of the core data protection principles, as identified by the WP29 in their working document WP254, can be found in their entirety in the Vietnamese legal system, although parts of them are included. For example, LCIS contains provisions on a legal basis for data processing, confidentiality, purpose limitation, and restrictions on data storage, as well as provisions on certain data subject rights such as the right

[290] Benjamin Greze, 'The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives' (2019) Vol 9, No 2 International Data Privacy Law, 109.

to access, rectification, and object against data processing. Nevertheless, as pinpointed in section 3.3 of this paper, in comparison with GDPR, the provisions in LCIS run short on details, and additionally, do not applies to state agencies.[291]

In *Schrems* case, CJEU clarified that a third country's data protection regime must not be identical to the one in the EU, and the means resorted to may differ. However, the bar for an adequacy decision was set to 'essentially equivalent' with the level of protection guaranteed in the EU, indicating that only minor deviations can be tolerated. Nevertheless, the threshold remains unclear as well as if all elements requested in a data protection regime, are of equal importance. Consequently, it is also uncertain what element, if any, a third country might be accepted not to have, and under what conditions. This lack of clarification as to how, and to what extent, the elements listed in Article 45(2) GDPR should be met entails several negative implications. Due to the lack of transparency, in particular, on the part of the Commission in not publishing its previous adequacy analysis, the methodology for adequacy has been rightly criticized.[292]

Firstly, the absence of clear references of how adequacy requirements are weighted gives leeway for political considerations by the European Commission in its assessment on adequacy. As long as certain parts of the adequacy procedure are kept untransparent, it cannot be ruled out that the Commission, based on the country in question, act biased and applies a more or less rigorous assessment based on political considerations. Thus, a benevolent approach can be adopted towards a country where there is a very strong financial interest in facilitating cooperation, whereby some shortcomings may be disregarded in favor of the conclusion that the country's data protection regime is adequate. Contrariwise, some flaws may be given

[291] See LCIS, arts 16-18.
[292] See Makulilo A. B, 'Data Protection Regimes in Africa: Too Far from the European "Adequacy" Standard?' (2013) 3 International Data Privacy Law 42.

improper importance to exert legal pressure against a country who desires an adequacy decision, but with which the EU has no greater interest in.

A second implication of the fact that the adequacy assessment partly lacks insights is that it is impossible for a country to ascertain beforehand whether it fulfills the adequacy requirements or not. Without further clarifications from the European Commission, it can never be clear enough if a country's level of data protection will be adjudged as essentially equivalent to the level in the EU. Moreover, the adoption of an adequacy decision will remain as an entirely hypothetical issue.

In substantive terms, Vietnam has established a data protection regime that partly matches the data protection regime in the EU. Despite the lack of a horizontal data protection law, most of the principles listed in WP254 can be found in sectoral legislation in Vietnam, which includes data protection rules. In this regard, LCIS and LIT have proven to be the most comprehensive, and they contain data protection concepts, principles for data processing, data subjects' rights, and provisions on legal remedies. However, counterparts to the principles of special categories of data (sensitive data) and restrictions for onward transfers are missing in the Vietnamese legal system. This raises the question of whether these shortcomings preclude the adoption of an adequacy decision in relation to Vietnam since they are essential elements of the GDPR and, additionally, highlighted in WP254.

In terms of GDPR's concept of special categories of data, it can be recalled that Article 9 of GDPR prohibits the processing of some data considered sensitive unless certain situations for derogations apply. For instance, an exception can be made if the data subject explicitly consents to the processing or if the processing is necessary for reasons of substantial public interest and the processing is proportionate and safeguards for the fundamental rights of the data subject's is provided. A similar restriction of the processing of sensitive data cannot be found in Vietnam's legal system. However, Article 17 of LCIS only recognizes consent and request by public authorities as

legitimate bases for the processing of personal data, whether it is sensitive or not. Therefore, one could argue that the protection of sensitive data, after all, should be considered sufficient in Vietnam. On the other hand, an authority's request to access personal data do not have to be in the public interest or proportionate, whereupon the opposite conclusion also can be drawn. Furthermore, and as previously shown, there are other sectoral laws in Vietnam that recognize more bases for data processing within their scope, which means that the protection of sensitive data in Vietnam may vary.

The principle of restriction on onward transfers may be considered essential for the entire EU data protection regime. The sole purpose of Chapter V of GDPR is to prevent that the level of data protection within the EU is undermined when data are transferred to third countries. However, without any rules restricting onward data transfers in the third country's legal system, the data protection required by GDPR for a data transfer from the EU can easily be adventured in a subsequent step. The importance of restrictions on onward transfers is therefore expressed, both in Article 44 GDPR, the overall provision for data transfers, as well as in Article 45 GDPR, the provision for adequacy decisions. Thus, in the absence of a restriction on onward transfers of data in Vietnam, the country is unlikely to be considered to have adequate data protection. On the other hand, this deficiency can easily be fixed by a statutory provision limiting personal data transfers from Vietnam without any assurance of the recipient's protection level.

4.2.2 Procedural deficiencies

As discussed in section 3.4 of this paper, the EU requires an independent data protection supervisory authority, a high level of compliance with data protection rules, accountability, and the existence of redress mechanisms in an adequate data protection regime. In terms of these procedural requirements, Vietnam shows significant deficiencies. To start with, the lack of an independent supervisory authority in Vietnam, with the task to ensure compliance with the country's data protection rules is a serious defect. Admittedly, Vietnam has two bodies tasked with monitoring regulatory

compliance in the field of information security, the MIC and the AIS. However, MIC is subject to a reporting obligation in relation to the National Assembly, putting it in a dependency position. This could affect the efficiency of MIC's data protection supervision, not least with regard to the National Assembly. The same applies to AIS, as this body is set up by MIC and can only act in accordance with the latter's instructions.

When the level of compliance and accountability were examined in relation to Vietnam's data protection regime, it was found that some of the measures WP254 states are likely to contribute to a high degree of compliance have been adopted in Vietnam. For instance, both LCIS and LIT establishes relatively harsh sanctions. Ignorance of their data protection rules can lead to rather high administrative fines or criminal penalties. WP254 suggests that severe penalties may have a dissuasive effect, but it is questionable whether such an effect is achieved in Vietnam. The reporting on enforced penalties in relation to data protection violations tells that sanctions are only imposed in a few cases, whereupon the penalties, regardless of their content, will not be deterrent for real. At the same time, statistics on the practice of punishment are not always made public in Vietnam, which makes it difficult to draw any certain conclusions. Admittedly, one could argue that this uncertainty in itself is daunting, as it remains unclear if and, in such case, how data protection infringements are punished. However, uncertainty in relation to crime convictions opposes the rule of law, which is a prerequisite for a decision on adequacy.

The existence of effective redress mechanisms is the final procedural requirement identified in WP254, and it encompasses the data subject's real opportunities to exercise their rights. Among other things, it concerns the availability of legal channels for petitions since the rights of data subjects only are real if they can be invoked. This raises the question of access to court in Vietnam. In terms of LCIS or LIT, both laws lack detailed provisions on ways to exercise the right to remedies. As previously mentioned, Article 20 LCIS provides that state agencies are responsible for establishing online

information channels for receiving petitions. Further, LIT contains a general provision on dispute settlements, which encourages the use of conciliation. However, as to this moment, it shall be left unresponded if and in such a case how a data subject may bring legal action to court in Vietnam for violations of its right to privacy or data protection. Based on the international reporting referred to previously, which claimed that violations of the right to privacy at this moment occur in Vietnam, this uncertainty about the existence of effective legal remedies impedes a decision on adequacy.

4.3 Final considerations

After a thorough review of the EU requirements for adequacy, especially as they have been elaborated by CJEU and WP29, in parallel with a survey of Vietnam's data protection regime, the following can be noted. *First,* the EU requirements for an adequacy decision has not yet been specified in terms of its practical application to such an extent that it is possible to determine with certainty whether a country meets the requirements. *Second,* the Vietnamese legal system contains several of the legal elements that Article 45 GDPR requires for adequacy, especially in substantive terms, but lacking counterparts to most of the EU requested procedural mechanisms. *Finally,* there is currently a gap between the EU requirements and the Vietnamese legal system in the context of adequacy, and arguably it is wide due to the legal reality in Vietnam. The picture that emerges from the Vietnamese regulations does not match the information given by legal practitioners, whereby no amendments in law is enough to close the gap.

Lists of materials

Table of Statues, Conventions and Preparatory Work

European Union

Hard law

Charter of Fundamental Rights of the European Union [2016] OJ C 202/389 (EU Charter).

Consolidated version of the Treaty on European Union [2016] OJ C 202/13 (TEU).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (Data Protection Directive).

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

Framework agreement on comprehensive partnership and cooperation between the European Union and its Member States, of the one part, and, the Socialist Republic of Vietnam, of the other part [2016] OJ L 329/8 (PCA).

European Commission

Commission, *The economic impact of the EU-Vietnam agreement, 1 January 2017 – 31 December 2017* (Luxemburg: Publications Office of the European Union, 2018) <https://trade.ec.europa.eu/doclib/docs/2019/february/tradoc_157686.pdf> accessed 7 January 2020.

Commission, 'Proposal for a Council Decision on the conclusion of the Free Trade Agreement between the European Union and the Socialist Republic of Viet Nam' COM (2018) 691 final (FTA).

Commission, 'Proposal for a Council Decision on the conclusion of the Investment Protection Agreement between the European Union and its Member States, of the one part, and the Socialist Republic of Viet Nam, of the other part' COM (2018) 693 final (IPA).

European Parliament

European Parliament, Legislative train 10.2019, 3 International Trade – INTA, *EU-Vietnam free trade agreement (EVFTA)* <www.europarl.europa.eu/legislative-train/api/stages/report/10-2019/theme/international-trade-inta/file/eu-vietnam-fta> accessed 7 January 2020.

European Parliament resolution of 15 November 2018 on Vietnam, notably the situation of political prisoners (2018/2925(RSP)).

Article 29 Working Party Documents (WP29)

Article 29 Data Protection Working Party, 'Working Document 01/2016 on the justification on interference with the fundamental right to privacy and data protection through surveillance measures when transferring personal

data (European Essential Guarantees)' (Adopted on 13 April 2016) (WP237).

Article 29 Data Protection Working Party, 'Adequacy Referential (updated)' (Adopted on 28 November 2017) (WP254).

Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (As last Revised and Adopted on 11 April 2018) (WP260 rev.01).

European Data Protection Board (EDPB)

European Data Protection Board, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation'(16 November 2018), 3 <www.edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en> accessed 2 December.

European Data Protection Board, 'Endorsement of GDPR WP29 Documents' (25 May 2018) <www.edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en> accessed 24 November 2019.

Vietnam

Civil Code, No. 91/2015/QH13.

Constitution of the Socialist Republic of Vietnam (The National Assembly, 28 November 2013, Hanoi) (Vietnam's Constitution).

Criminal Code, No. 100/2015/QH13.

Cybersecurity Law, No. 24/2018/QH14 (CSL)

Law on Insurance Business, No. 24/2000/QH10 as amended by Law No. 61/2010/QH12.

Decree amending and supplementing a number of articles of the government's decree no. 90/2008/ND-CP dated August 13, 2008 on Anti-spamming (No. 77/2012/NĐ-CP) October 05, 2012.

Decree on Information Technology application in State Agencies' operations, No. 64/2007/ND-CP.

Law on Credit Institutions, No. 47/2010/QH12.

Law on Cyberinformation Security, No. 86/2015/QH13 (LCIS).

Law on E-Transactions, No. 51/2005/QH11.

Law on Information Technology, No: 67/2006/QH11 (LIT).

Law on Protection of Consumers' Rights, No.59/2010/QH12.

International Law

The Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108).

UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999.

UN General Assembly, Universal Declaration of Human Rights, 10 December 1948.

Other

ASEAN Telecommunications and information technology ministers meeting (Telmin), 'Framework on personal data protection' <https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf> accessed 28 December 2019.

Delegation of the European Union to Vietnam, Guide to the EU-Vietnam Trade and Investment Agreement (Guide to EU-Vietnam agreements) (Updated in March 2019) <https://eeas.europa.eu/sites/eeas/files/eu_fta_guide_final_3.pdf> accessed 20 November 2019.

Cases

Joined C 584/10 P, C 593/10 P and C 595/10 P *European Commission and Others v Yassin Abdullah Kadi* [2013] EU:C:2013:518.

Joined cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, Irish Human Rights Commission (intervener), and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others [2014] ECLI:EU:C:2014:238 (Digital Rights Ireland).

Case 362/14 *Maximillian Schrems v Data Protection Commissioner, Digital Rights Ireland Ltd.* (*Schrems* case) [2015] EU:C:2015:650.

Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] EU:C:2016:779 (*Breyer* case).

Case 311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian *Schrems* with others [2019] EU:C:2019:1145, Opinion of AG Saugmandsgaard Øe (*Schrems II* case).

Bibliography

Books

Hồng Quỳ M and others (eds), *Introduction to Vietnamese Law* (Hong Duc Publishing House– Viet Nam Lawyers Association 2015).

Kugler T and Rücker D (eds), *New European General Data Protection Regulation: A Practitioner's Guide* (Bloomsbury Collections 2018) .

Peczenik A, 'Legal doctrine and legal theory' in Corrado Roversi (eds), *A Treatise of Legal Philosophy and General Jurisprudence* (Springer, Dordrecht, 2005).

Riesenhuber K (ed), *European Legal Methodology* (Ius Communitatis, 1st edn, vol 7, Intersentia, 2017).

Articles

Danwitz T, 'The Rule of Law in the Recent Jurisprudence of the ECJ' (2014) Vol 37, No 5 Fordham International Law Journal, 1311.

Estey W, 'The Five Bases of Extraterritorial Jurisdiction and the Failure of the Presumption against Extraterritoriality' (1997) Vol 21, No 1, Hastings International and Comparative Law Review, 3.

Greze B, ‘The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives’ (2019) Vol 9, No 2 International Data Privacy Law, 109.

Hintze M, ‘Viewing the GDPR through a de-identification lens: a tool for compliance, clarification, and consistency’ (2018) Vol 8, No 1 International Data Privacy Law, 86.

Kokott J, ‘The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR’ (2013) Vol 3, No 4 International Data Privacy Law, 222.

Kuner C and others, ‘The language of data privacy law (and how it differs from reality)’ (2016) Vol 6, No 4 International Data Privacy Law, 259.

Kuner C and others, ‘The GDPR as a chance to break down borders’ (2017) Vol 7, No 4 International Data Privacy Law, 231.

Makulilo A. B, ‘Data Protection Regimes in Africa: Too Far from the European “Adequacy” Standard?’ (2013) 3 International Data Privacy Law 42.

Moerel L, ‘The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?’ (2011) Vol 1, No 1 International Data Privacy Law, 28.

Slokenberga S and others, ‘EU data transfer rules and African legal realities: is data exchange for biobank research realistic?’ (2019) Vol 9, No 1 International Data Privacy Law, 30.

Santa Slokenberga, Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal and Tunisia. Adequacy considerations and Convention 108, IDPL pending approval after peer-review (unpublished).

Wagner J, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) Vol 8, No 4 International Data Privacy Law, 318.

Miscellaneous

ASEAN Insiders Series 2019 – Personal Data Protection, see rubric 'ASEAN Data Protection Laws & Readiness for EU GDPR' (19 July 2019) <https://asialawportal.com/2019/07/19/asean-insiders-series-2019-personal-data-protection/> accessed 28 December 2019.

Cooper G and Le H, 'Vietnam's new Cybersecurity Law: A headache in the making?' (Cecile Park Media, 2018) <www.duanemorris.com/articles/static/cooper_le_cybersecurity_practitioner_0718.pdf> accessed 23 November 2019, 14-15.

Data protected Vietnam, see rubric 'Practice' <www.linklaters.com/en/insights/data-protected/data-protected---vietnam> accessed 24 December 2019.

Data Protection in Vietnam: Overview, see rubric 'Enforcement and sanction,' Question 25 <www.amchamvietnam.com/wp-content/uploads/2019/05/Data-Protection-in-Vietnam-Overview-April-2019.pdf> accessed 24 December 2019.

David Törngren, Explanatory notes to GDPR 2016, art 2, (Karnov, 1 June 2018) <https://pro-karnovgroup-se.ludwig.lub.lu.se/document/2514469/1> accessed 15 September 2019.

Joint NGO Call to Postpone Consent to EVFTA and IPA (Brussels, 4 November 2019) <www.icj.org/wp-content/uploads/2019/11/Vietnam-EVFTA-Advocacy-open-letters-2019-ENG.pdf> accessed 30 December 2019.

Minor Field Studies, <www.utbyten.se/program/minor-field-studies/> Accessed 7 January 2020.

Rouse The Magazine, 'Vietnam: Three new important regulations on data protection in the making' <www.rouse.com/magazine/news/vietnam-three-new-important-regulations-on-data-protection-in-the-making/> accessed 30 December 2019.

The Official webpage of the Ministry of Information and Communication of the Socialist Republic of Vietnam, 'Main functions' <http://english.mic.gov.vn/Pages/ThongTin/114253/Main-Functions.html> accessed 23 December 2019.

The official website of the Council of Europe, 'Charts of signatures and ratifications of Treaty 108' <www.coe.int/en/web/conventions/full-list//conventions/treaty/108/signatures?p_auth=g1E83e21> accessed 27 December 2019.

The official website of the European Commission, 'Countries and regions, Vietnam' <https://ec.europa.eu/trade/policy/countries-and-regions/countries/vietnam/> Accessed 20 November 2019.

Thư viện pháp luật (Lawsoft) <https://thuvienphapluat.vn/> accessed 31 December 2019.

Utrikespolitiska institutet, Landguiden Vietnam <www.ui.se/landguiden/lander-och-omraden/asien/vietnam/> accessed 7 January 2020.