The Legal Protection of International Organisations' Data

Study of the Big Data Program to Implement the UN Sustainable Development Goals with Regard to EU and Chinese Data Protection Laws

LEIDEN ASIA CENTRE
Partners in Research and Knowledge

CKN China Kennisnetwerk

Aude Géry & Anne-Thida Norodom

January, 2023

The research for and production of this report has been conducted within the framework agreement for the Chinese Knowledge Network (CKN). The aim of CKN is to promote strategic knowledge development about China for the national government of the Netherlands. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the secretariat of the Chinese Knowledge Network and/or the Netherlands Ministry of Foreign Affairs.

The LeidenAsiaCentre is an independent research centre affiliated with Leiden University and made possible by a grant from the Vaes Elias Fund. The centre focuses on academic research with direct application to society. All research projects are conducted in close cooperation with a wide variety of partners from Dutch society.

More information can be found on our website:

www.leidenasiacentre.nl

For contact or orders: info@leidenasiacentre.nl

M. de Vrieshof 3, 2311 BZ Leiden, The Netherlands

Contents

Foreword (Rogier Creemers)

China's ambitions to achieve global leadership in big data have become well known. One less prominent aspect of these plans is that China has worked together closely with the UN in linking data processing and analysis capabilities with the realization of the 2030 Sustainable Development Goals.

Specifically, in October 2014, the UN Department of Economic and Social Affairs (UNDESA) launched a collaboration with China's National Bureau of Statistics (NBS) on big data in official statistics. This led, in 2019, to the signature of a letter of intent between NBS and UNDESA concerning cooperation in capacity building on big data and governance in the developing world. This would create a regional hub integrating with an earlier collaborative initiative between the UN and the UK National Statistics Office to build the "United Nations Global Platform" . This regional hub is intended to provide technical assistance and capacity building in the use of big data for SDG indicators, leveraging China's technical expertise to assist other countries in the region. As a knowledge centre, it is intended to assist in the development of a broader network of national, regional and global data hubs, provide training materials and information sharing. Lastly, it is intended to act as a technology and innovation hub, establishing links with relevant research institutions and think tanks and convening technical seminars and symposia to further collaboration between partner countries. The first personnel was in place by May 2020. This regional hub is located in the Hangzhou Big Data Centre, and the NBS has even released a floor plan of its office buildings .

For China, this regional hub provides an opportunity to showcase the progress of its digital prowess, but for other countries, this raises questions. Although, over the past few years, China has developed a rapidly growing regulatory framework for data protection, this leaves wide discretion to government bodies . The 2017 National Intelligence Law requires all Chinese entities and individuals to cooperate with intelligence services, ostensibly requiring the provision of access to data or restricted facilities . Previous reporting on Beijing's potential access to Apple's data centres in China , as well as the country's well-known cyber espionage operations have generated apprehensions among foreign governments and analysts about the security of data stored in this UN regional hub as well.

Nonetheless, assessing the security of this data centre, or other joint initiatives between the UN and Beijing, involves multiple levels. Basic technical components of security, including encryption and access control for authorized users, can only be evaluated through a thorough investigation, preferably involving cooperation from the operators involved. China's track record here is spotty: in the summer of 2022, a hack of the Shanghai police database became public knowledge, with hackers claiming they had obtained a dataset on over a billion individuals. This followed leaks of the personal information of over two million Communist Party members in Shanghai, and facial recognition information of thousands of Beijing residents . Political considerations are also involved, both at the domestic and international levels. If the regional hub were to be hacked by Chinese intelligence services, it would likely cause significant embarrassment for the NBS within the system, as well as for the Chinese government globally. This would contravene China's demonstrated intention to increase its "discursive power " and influence in the UN system. From the legal angle, as mentioned above, legislation poses few constraints to the operations of Chinese government entities. However, domestic law is not the only applicable rule-setting framework in this area. The UN is, after all, an international governmental organization, which means international law applies as well.

The interface between existing international law and data protection where international organizations are concerned, is an area that nonetheless has largely remained out of the spotlight thus far. This report, therefore, intends to contribute an exploratory analysis of specifically what international law doctrine has to offer on the obligations and prohibitions placed on national governments in their engagement with UN-held data.

Executive summary

This study deals with the legal protection of international organisations' data that may be stored in China. It is part of a research project on the impact on Dutch data security of data storage in China. One of the main lines of this research project is the question to what extent China-based data storage by the UN meets Dutch/EU legal requirements with regard to privacy and cybersecurity.

The data of Europeans transferred to the United Nations is likely to be stored in China or to be entrusted, as part of a cloud offer, to a Chinese service provider.

In June 2019, the UN Department of economic and social affairs signed a letter of intent with the National Bureau of Statistics of China for the creation of a regional hub for big data in support of the United Nations Global Platform, a cloud-service ecosystem to support international collaboration in the development of statistics.[1] The regional hub includes 700 m^2 of servers and aims at developing the use of big data for statistics in the context of the 2030 Agenda for Sustainable Development.

However, this does not imply that Chinese (or European) law applies to the data once it is transferred to the UN because of the privileges and immunities of the UN and the prevalence of member states' obligations under the Charter (Art. 103 of the Charter). This means that the Chinese government cannot access UN data, unless explicitly authorized to do so. In the event of unauthorized access, the United Nations could seek to hold China responsible.

Even though under EU and Chinese data protection law, international organisations could be considered as data controllers and subject to the obligations contained in these instruments, they have a special status under general international law which exclude them from the scope of application of these national regulations. UN digital data can be qualified as "property and assets"[2] and as such, enjoy immunity from any form of interference, regardless of where it is stored or how it is stored. This immunity from legal process is accompanied by an absolute inviolability for United Nations archives and documents, including ICT data. If the data is held and stored by the organisation itself, on its own server for example, the qualification of

[1] https://unstats.un.org/bigdata/regional-hubs/china-concept-note.pdf

[2] Letter from M. de Serpa Soares to A. Jelinek, 14 May 2020, p. 14, para. 38. See also UN Joint Inspection Unit Report Cybersecurity in the United Nations system organizations, JIU/REP/2021/3, p. 2, para. 5; p. 41, para. 168.

"premises of the organization" could apply and these infrastructures would benefit from inviolability as such.[3] Thus, the regional centres established under the UN Global Platform programme, including the regional centre located in China, could be qualified as premises of the organisation.

Recommendation: The conclusion of an agreement between China and the UN on the Regional Centre for the UN Global Platorm should be encouraged or, if it already exists, ensure the recognition of the immunities of the stored data and the inviolability of this Regional Centre.

The non-applicability of European or Chinese law does not mean that there is no legal framework for data within the UN system. However, as it stands, it does not appear that the level of data protection by the UN is equivalent to the European level.

The UN has produced a set of internal rules and policies relating to data protection. These principles are very similar to those that can be found in the GDPR or the PIPL and are part of what can be called today the common law of personal data protection. However, they are very vague and need to be interpreted. The current interpretation seems to favor the specific purpose of data processing by the UN to justify a more liberal approach to data protection than the European one.

Recommendation: The development of a more precise data protection framework within the United Nations should be encouraged in order to ensure a level of protection equivalent to other data protection systems, notably European, and thus facilitate the international transfer of personal data.

The UN process a multitude of data. As EU and Chinese laws are developing in the field of data protection (and not only of personal data), the conflict of laws between the EU and China on one hand and the UN on the other hand are likely to increase.

Recommendation: In order to ensure the appropriate level of protection of its citizens' data, the continuation of the discussions between the EU and the UN on data transfer should be encouraged to better anticipate the normative developments resulting from the European Data Strategy, in particular the DGA and the Data Act.

Technical and contractual measures can be taken to ensure the appropriate level of protection of UN data, including in the context of cloud computing services.

[3] Article II, section 3 of the Convention on the Privileges and Immunities of the United Nations.

Recommendation: The adaptation of contracts between the UN and cloud service providers should be encouraged to match the specificities of UN data. In particular, it should be ensured that there are specific security obligations for the hosting provider to ensure the physical and IT security of UN data.

Introduction

This study deals with the legal protection of international organisations' data that may be stored in China. It is part of a research project on the impact on Dutch data security of data storage in China. One of the main lines of this research project is the question to what extent China-based data storage meets Dutch/EU legal requirements with regard to privacy and cybersecurity. In June 2019, the UN Department of economic and social affairs signed a letter of intent with the National Bureau of Statistics of China for the creation of a regional hub for big data in support of the United Nations Global Platform, a cloud-service ecosystem to support international collaboration in the development of statistics.[4] The regional hub has been built and includes 700 m^2 of servers and aims at developing the use of big data for statistics in the context of the 2030 Agenda for Sustainable Development. As a consequence, Dutch data transferred to the UN may be stored in China. Understanding the consequences of such decision for the Netherlands and the EU members thus requires studying the interactions between the United Nations and EU and Chinese laws. The legal analysis will therefore have two dimensions: on the one hand, the data protection of international organisations, and on the other hand, the comparison of the requirements of EU law and Chinese law with regard to the protection of such data.

The applicable law on data protection is manifold. There are general legal instruments relating to the international protection of human rights, which do not deal directly with data protection, but which may apply, such as the International Covenant on Civil and Political Rights. There are also a growing number of specific international legal instruments on data protection, both binding (General Data Protection Regulation - GDPR) and non-binding (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data). The existence of this international data protection body of law does not prevent States from adopting their own national legislation in this field. In addition to this multiplicity of applicable sources of law, there is also a multiplicity of legal instruments due to the diversity of data.

In the context of this study, the chosen perspective thus confronts three normative corpuses applicable to the data examined in this study: that of the European Union, that of China and that of international organisations. In terms of digital law, and more specifically in terms of

[4] https://unstats.un.org/bigdata/regional-hubs/china-concept-note.pdf

data protection and cybersecurity, the European Union and China are based on different logics, even if they may use common terminology. In simple terms, the European data protection system[5] is based on a personalist logic of data, where data is attached to the human person and should therefore be fundamentally protected, within a liberal economic system. The Chinese personal data protection system[6] is more focused on the protection of national security. These two approaches are opposed by a third approach, that of international organisations, which benefit, under international law, from a special legal status to protect the exercise of their functions.

This study will focus on the data of the United Nations (UN), a classic intergovernmental organisation,[7] based on a treaty, the Charter, and endowed with international legal personality, *i.e.* "a subject of international law and capable of possessing international rights and duties, and that it has capacity to maintain its rights by bringing international claims."[8]

The study of the United Nations is particularly interesting because this organisation has an extremely rich body of specific law (primary law stemming from the Charter and secondary law produced by its principal and subsidiary organs), a highly developed operational activity dedicated to the maintenance of international peace and security (involving the collection and processing of extensive data), and legal instruments of its own, such as the Convention on the Privileges and Immunities of the United Nations.[9] Much of the reasoning in this note will be at least partially applicable to organisations belonging to the UN system as a whole,[10] subject to the application of the internal law of each organisation. Indeed, even if there is a common

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[6] This system is based in particular on the Personal Information Protection Law of the People's Republic of China, Chairman's order N°91, which was adopted by the 30th meeting of the Standing Committee of the 13th National People's Congress of the People's Republic of China on August 20, 2021 and came into force as of November 1, 2021.

[7] Art. 2(a), Articles on the Responsibility of International Organizations.

[8] *Reparation for injuries suffered in the service of the United Nations*, Advisory Opinion: *I.C.J. Reports 1949*, p. 179.

[9] Convention on the Privileges and Immunities of the United Nations (1946), United Nations, *Treaty Series*, vol. 1, p. 15, and vol. 90, p. 327 (corrigendum to vol. 1); Convention on the Privileges and Immunities of the Specialized Agencies (1947), United Nations, *Treaty Series*, vol. 33, p. 261.

[10] See: https://www.un.org/en/pdfs/un_system_chart.pdf

logic to all the organisations of the UN system, in particular in the field of data protection,[11] each organisation has its own constitutive treaty, its own internal and external law and often its own data protection practices. The developments that follow may thus change according to the legal nature of the international institution in question. Considering the variety of international organisations,[12] the study of each of these organisations, as well as other international institutions outside the UN system, would require adapting our analysis to the specific law of each organisation and the specific legal instruments that may apply.

Data is a representation of information. It can be personal, economic, sensitive, security-related, etc. The data of international organisations are therefore extremely numerous and diverse, and are susceptible to multiple legal qualifications. The issue of the legal qualification of data is central since it will make it possible to identify the applicable legal regime.

Structure of the paper

This study focuses on the digital data of international organisations and more specifically of the UN in the context of its work on big data and Sustainable Development Goals. As the data in question is likely to be stored in China, the legal analysis will be geographically dynamic by considering the issue of data transfer from China and consequently the compatibility between Chinese law and European law

In a Part 1, we will specify the context in which UN data are produced, and more precisely the role of big data in the UN program of work. We will see that because data plays a big role in the way the UN fulfill their functions, China may be involved in numerous ways. This first section will set the scene to later identify these data and the legal issues, at the intersection of data protection law and the law of international organisations, that their processing raise.

In Part 2, we will look at how the law of international organisations opposes the application of both EU and Chinese law to UN data while organizing a specific regime for data protection. This has twofold consequences. On the one hand, it implies that States, including China, must

[11] See for ex., the UN Privacy Policy Group, an inter agency group, whose the objectives are to advance dialogue and information sharing on key issues related to data privacy and protection within the UN system but also the System-wide Road Map for Innovating United Nations Data and Statistics, CEB/2020/1/Add.1, 14 May 2020

[12] E. Lagrange, "La catégorie 'organisation internationale'", *in* E. Lagrange and J.-M. Sorel (eds.), *Traité de droit des organisations internationales*, LGDJ, 2013, p. 43-62.

not access any UN data without appropriate authorization from UN authorities. On the other hand, it means that any data, including data coming from the EU territory, and wherever it is located, is subject to a specific UN data protection legal framework.

Finally, Part 3 of the paper will focus on the different precautions, that, despite its immunities, the UN should take to better protect its data. These two lines of efforts are of two kinds and will benefit European data. Firstly, because of the diversity of data and its multiple origins, more and more European and Chinese laws are likely to seek to apply to UN data. The UN should therefore seek to develop a comprehensive and protective data regime. Secondly, even though UN data is immune, several elements must be taken into account to secure data in the cloud, including when drafting the contract between the UN and the service provider.

Part 1: The Context of Data Production by the UN

1. Digital transformation through data and the use of Big Data

The United Nations is promoting digital transformation through data[13] and the use of Big Data[14] to enable the Organisation to fulfil its functions. The use of Big Data should thus facilitate the implementation of the UN Sustainable Development Goals (SDGs)[15].

There is a UN Committee of Experts on Big Data and Data Science for Official Statistics composed of task teams, whose objectives are to: "(a) negotiate, at the global level, access to data sources of private data owners, strictly to be used for statistical purposes to inform policies at the national, regional and global levels, especially to advance the implementation of the 2030 Agenda for Sustainable Development; (b) demonstrate through use cases the relevance of these data sources for statistical purposes; and (c) advise on institutional arrangements after the completion of successful experimentation and testing."[16]

There are also two interesting initiatives:

- One general, the UN Global Pulse, which "promotes awareness of the opportunities big data presents for sustainable development and humanitarian action" and "set up a Data Privacy Advisory Group, comprised of privacy experts from the regulatory community, private sector and academia, that engages in dialogue on the critical issues around big data and advises on the development of privacy tools and guidelines across the UN;"[17]

[13] Report of the Independent Expert Advisory Group on a Data Revolution for Sustainable Development: https://www.undatarevolution.org/wp-content/uploads/2014/11/A-World-That-Counts.pdf

[14] UNSG Data Strategy, p. 34.

[15] https://www.un.org/en/pdfs/Bigdata_SDGs_single_spread_2017.pdf ; https://unstats.un.org/bigdata/index.cshtml

[16] Report of the Committee of Experts on Big Data and Data Science for Official Statistics, 2022, E/CN.3/2022/25, p. 3, para. 5. https://unstats.un.org/bigdata/documents/reports/UNCEBD%20report%20-%202022-25-BigData-E.pdf

[17] https://www.un.org/en/global-issues/big-data-for-sustainable-development. The UN Global Pulse has initiated two documents: the Data Privacy, Ethics and Protection Guidance Note on Big Data for Achievement of the 2030 Agenda, November 2017

- The other more operational, the UN Global Platform, which is a "cloud-service ecosystem to support international collaboration in the development of Official Statistics using new data sources and innovative methods and to help countries measure the Sustainable Development Goals (SDGs) to deliver the 2030 Sustainable Development Agenda."[18]

As part of this policy to promote Big Data, the UN has set up four regional centers whose objective is to "educate, collaborate and develop new technologies to work with new Big Data sources and methodologies."[19] One of these centers is in China[20], with 700 m² of servers.[21]

The UN also has a UN International Computing Centre (ICC) which provides IT services and solutions, including IT security. It has several offices around the world[22] and four data centers located in Geneva (Switzerland), Valencia (Spain), and Piscataway (NJ, USA). Its operation appears to be unique in that it requires contracts between the organisation and the ICC.[23]

(https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf) and the Personal Data Protection and Privacy Principles, adopted by the UN High Level Committee on Management on 11 October 2018.

[18] https://unstats.un.org/bigdata/un-global-platform.cshtml

[19] https://unstats.un.org/bigdata/regional-hubs.cshtml#china

[20] It is not clear why China was chosen to host this center. However, it can be said that it is in line with its strategy to present itself as a major player in multilateralism. Furthermore, China has long cooperated with the UN in the field of statistics and big data. For example, in 2009, the UN-China Trust Fund Project on Statistical Capacity Building was established with the objective of developing China's statistical capacity. In 2014, China hosted the first International Conference on Big Data and Official Statistics organized by the Department of Economic and Social Affairs. It has thus been an important player in the UN's work in this area from the beginning. Finally, its capacities developed in this field could be seen as an asset to train, at the regional level, other States in the field of statistics and big data and thus strengthen the big data and SDG program. It must be noted that, in September 2021, China has opened, within the Chinese Academy of Science, the International Research Center of Big Data for Sustainable Development Goals that will work closely with the regional hub established in Hangzhou.

[21] https://unstats.un.org/bigdata/regional-hubs.cshtml#china

[22] According to the UN ICC website, it has established offices in Geneva, Switzerland; Valencia, Spain; Brindisi and Rome, Italy; and New York, USA. It also has a presence in Madrid, Spain and in the Green One UN House in Hanoi, Vietnam.

[23]United Nations, *Managing cloud computing services in the United Nations system*, Report of the Joint Inspection Unit, prepared by Jorge T. Flores Callejas and Petru Dumitriu, JIU/REP/2019/5, pp. 48-49.

2. The use of data for the implementation of the SDGs.

Data are used by the Statistics Division in order to develop the SDGs Global Database. They come from a wide range of sources. The Metadata Repository details, for each indicator, the type of data being used and its origin. A study of the different indicators shows that data either come from other international organizations or directly from States and non-state actors[24] .

Data used in this context are not homogeneous and cannot be apprehended in the same way: the legal protection might differ depending on the type of data and the conditions regarding the transfer of data might differ as well, depending where they come from.

Thus, there are several types of data for the implementation of the SDGs alone. Examples include:

- Data on national legislation. Ex : Indicator 12.1.1: Number of countries developing, adopting or implementing policy instruments aimed at supporting the shift to sustainable consumption and production;
- Statistical data. Ex: Indicator 10.7.4: proportion of the population who are refugees, by country of origin. This is not data on refugees but statistics on data available to the United Nations High Commissioner for Refugees.

Further study would require more precise information from the UN on the data mobilised in the context of the implementation of the SDGs.

3. Data storage outsourcing strategy

The COVID crisis seems to have encouraged or accelerated the strategy of outsourcing data storage to the cloud.[25]

There are different types of clouds:

[24] https://unstats.un.org/sdgs/metadata/. The metadata repository describes the type of data and statistics used for the Tier I and II indicators in the global SDG indicator framework.

[25] *Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity 2020-2022*, May 2020, p. 34.

- Clouds can be differentiated according to the level of outsourcing, from the lowest to the highest: IaaS (Infrastructure as a Service); PaaS (Platform as a Service); SaaS (Software as a Service);
- They can also be categorized according to their deployment mode: private, community/hybrid, public cloud.

Depending on the type of cloud used, the degree of customer control over the service will vary.[26] It is therefore important to tailor the contract between the UN and the cloud provider to the characteristics of the chosen cloud.

UN data is multifaceted in its purpose and may involve China in various ways. The data may be stored in the context of the above-mentioned Chinese regional centre, through a cloud service with potentially Chinese service providers, without the location of the data necessarily being known. Finally, the data may have been transferred from an international organisation, a Member State or a non-State actor to the UN, which *a priori* contributes to the complexity of identifying the applicable law. The range of situations is extremely wide and could raise numerous legal issues. However, their spectrum can be reduced in view of the status of international organisations, which enjoy a unifying legal protection.

[26] For a clear description, see:
https://www.ifri.org/sites/default/files/atoms/files/bomont_cloud_defense_2021.pdf

Part 2: General Data Protection in Relation to the Status of International Organisations

1. Chinese law and EU data protection law

Both Chinese and EU law have a set of rules applicable to data protection, whether personal or not. If we take the example of personal data protection law, both Chinese and EU law impose obligations on data controllers, whether they are natural or legal persons. According to these laws, organisations could be therefore affected by these rights and obligations.

With regard to Chinese law:

- Art. 10 PIPL: "No *organization* or individual may illegally collect, use, process, or transmit personal information, or illegally trade, provide, or disclose other personal information, or engage in the processing of personal information that endangers the national security or public interest;"
- Art. 42 PIPL: "For any overseas *organization* or individual whose personal information processing activities damage the personal information rights and interests of citizens of the People's Republic of China, or endanger the national security or public interests of the People's Republic of China, the State cyberspace administration may include such overseas organization or individual in the list of restricted or prohibited provision of personal information, announce the same, and take measures such as restricting or prohibiting the provision of personal information to such overseas organization or individual;"
- Art. 65 PIPL: "Any *organization* or individual has the right to complain or report illegal personal information processing activities to the departments performing duties of personal information protection (...)."

With regard to European Union law:

- Art. 4(7) GDPR : "'controller' means the natural or *legal person*, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing; where the purposes and means of the processing are determined by Union law or the law of a Member State, the controller may be designated or the specific criteria for such designation may be laid down by Union law or by the law of

a Member State", the same applies to processors, recipients, third parties, all of whom may be natural or legal persons (Art. 4(8), (9), and (10) GDPR).

- Chapter V: "Transfers of personal data to third countries and *international organisations*". It is curious, as the UN Legal Counsel has pointed out[27] , that the GDPR treats third states and international organisations in the same way, while under international law the latter do not enjoy the same status as the former.

Under specific personal data protection law, international organisations could be considered as data controllers and subject to the obligations contained in these instruments.

International organizations may also fall within the scope of other relevant Chinese laws.[28] Two types of provisions can be pointed out. On the one hand, some laws will explicitly set out the obligations of any "organization" (which could include international organisations).[29] Chapter VI of the 2015 National Security Law lists the "Duties and Rights of Citizens and Organisations".[30] 2021 Data Security Law and 2016 Cybersecurity Law establish a regime of liability in the event of a breach of these obligations[31] and the possibility to adopt sanctions against "foreign institutions and organizations" engaged in activities "endangering the

[27] Letter from M. de Serpa Soares to A. Jelinek, 14 May 2020, p. 19, para. 52.

[28] National Intelligence Law, adopted at the 28th session of the Standing Committee of the 12th National People's Congress on June 27, 2017; amended in accordance with the "Decision on Amending the P.R.C. Frontier Health and Quarantine Law and Five Other Laws" by the 2nd session of the Standing Committee of the 13th National People's Congress on April 27, 2018, Art. 11, 14; 2015 National Security Law, passed on July 1, 2015 at the 15th meeting of the Standing Committee of the 12th National People's Congress, Art. 77-79, 82; 2016 Cybersecurity Law, adopted on November 7, 2016, Art. 12; 2021 Data Security Law, adopted at the 29th session of the Standing Committee of the 13th National People's Congress on June 10, 2021.

[29] See 2016 Cybersecurity Law, Art. 12.

[30] Under Art. 77, citizens and organizations shall perform several obligations "to preserve national security: (1) Obeying the relevant provisions of the Constitution, laws, and regulations regarding national security; (2) promptly reporting leads on activities endangering national security; (3) Truthfully providing evidence they become aware of related to activities endangering national security; (4) Providing conditions to facilitate national security efforts and other assistance; (5) Providing public security organs, state security organs or relevant military organs with necessary support and assistance; (6) Keeping state secrets they learn of confidential; (7) Other duties provided by law or administrative regulations. Individuals and organizations must not act to endanger national security, and must not provide any kind of support or assistance to individuals or organizations endangering national security."

[31] Respectively Art. 45-46 and Art. 59-74.

critical information infrastructure of the PRC" for example.[32] On the other hand, certain Chinese laws will establish general legal principles for the regulation of certain activities, particularly digital ones, while leaving room for interpretation when these activities are likely to endanger national security. This is the case of the PIPL (Art. 10, 36, 38, 40, 42), the Data Security Law (Art. 8) and the Cybersecurity Law (Art. 1, 10, 58).

In any case, Chinese law as well as European Law can provide provisions applicable to international organizations, which have a special status under general international law, that should exclude them from the scope of application of these national and European regulations.

2. The specificity of the status of international organisations

The EU Delegation to the UN acknowledged in a *Note Verbale* of July 2018 that the privileges and immunities of the UN prevent the application of EU data protection law to the UN, "including to its Funds, Programmes, subsidiary organs and Specialised Agencies", that "UN entities can process the data required in their functioning without being bound by EU law" and "[t]his is the case even if the relevant offices may be situated in the territory of a Member State such as for instance the Food and Agriculture Organisartion of the United Nations (FAO), headquartered in Italy".[33] The specificity of international organisations has also been recognised by the European Data Protection Board in its Guidelines on territorial scope.[34] Furthermore, according to Article 103 of the UN Charter the obligations of Member States under the Charter prevail over any other obligations of Member States, including the European Treaties.

The specificity of international organisations, with regard to their privileges and immunities, recognised by the European Data Protection Board, also applies under Chinese law. Chinese law must respect the special status of international organisations, including immunities and inviolability. These immunities are recognised for the UN under customary international law

[32] 2016 Cybersecurity Law, Art. 75.

[33] NV 2018/56 from the European Union Delegation to the United Nations to the United Nations Office of Legal Affairs, 3 July 2018.

[34] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), as adopted by the European Data Protection Board after public consultation on 12 November 2019, p. 23: "the application of the GDPR is without prejudice to the provisions of International law, such as the ones governing the privileges and immunities of... international organisations".

and are necessary for the exercise of its activity, which serves public interest needs and must be protected from external political pressure.

UN digital data can be qualified as "property and assets"[35] and as such, enjoy immunity from any form of interference, including by legislative action, according to Article 105 of the Conventions on the Privileges and Immunities of the United Nations and of its Specialised Agencies[36] . Under Article II, section 3, of the Convention on the Privileges and Immunities of the United Nations, the property and assets of the UN, "wherever located and by whomsoever held, shall be immune, from search, requisition, confiscation, expropriation and any other form of interference, whether by executive, administrative, judicial or legislative action". Under Article II, section 2, of the same Convention, "wherever located and by whomsoever held, shall enjoy immunity from every form of legal process except insofar as in any particular case it has expressly waived its immunity. It is, however, understood that no waiver of immunity shall extend to any measure of execution". Thus, the United Nations digital data is protected from any interference, regardless of where it is stored or how it is stored. The location of the server or the use of a cloud service does not justify the application of the law of the State (or organisation) with territorial jurisdiction. Because of the special status of international organisations, UN data stored on Chinese territory should escape the application of Chinese data protection law.

As M. de Serpa Soares, Under-Secretary-General for Legal Affairs and United Nations Legal Counsel, mentioned: "this immunity from legal process is accompanied by an absolute inviolability for United Nations archives and documents, enshrined in Article II, section 4, according to which '[t]he archives of the United Nations, and in general all documents belonging to it or held by it, shall be inviolable wherever located'".[37] Thus UN documents considered as ICT Data can be qualified as documents and archives.[38] In the same way as

[35] Letter from M. de Serpa Soares to A. Jelinek, 14 May 2020, p. 14, para. 38. See also UN Joint Inspection Unit Report Cybersecurity in the United Nations system organizations, JIU/REP/2021/3, p. 2, para. 5; p. 41, para. 168.

[36] Convention on the Privileges and Immunities of the United Nations (1946), *op. cit*; Convention on the Privileges and Immunities of the Specialized Agencies (1947), *op. cit.*

[37] Letter from M. de Serpa Soares to A. Jelinek, 14 May 2020, p. 15, para. 39.

[38] ST/SGB/2004/15 and ST/SGB/2007/5. See in the same sense, G. L. Burci: "While the purpose of UN Secretary-General's bulletins and similar administrative issuances is primarily of an internal managerial and accountability nature and while they have no direct legal effects on third parties, such bulletins do have an indirect influence on the implementation of the General Convention as evidence

above, the use of a cloud hosting service, whatever the type of cloud used (public/private/hybrid, infrastructure or application), cannot affect the inviolability of data, qualified as archives and documents, of the United Nations. Again, it is the nature of the object (property and assets or United Nations archives and documents), and not the location and method of holding, that will define the protection regime for such data.

If the data is held and stored by the organisation itself, on its own server for example, the qualification of "premises of the organization" could apply and these infrastructures would benefit from inviolability as such.[39] Thus, the regional centres established under the UN Global Platform programme, including the regional centre located in China, could be qualified as premises of the organisation. In this case, the obligations of the host State are both positive: to protect the said premises from any threat or disturbance prejudicial to their operation[40] and negative: the host State may not enter the premises without the organisation's authorisation. The organisation must, for its part, exercise control over its premises and the activities that take place there[41]. The content of these obligations may be specified in the headquarters agreement between the host State and the organisation. We have not been able to access the possible headquarters agreement between the UN and China for the establishment of the regional centre. In a concept note available on th UN website, it is being written that "NBS and UN DESA has reached basic consensus on the MOU content after rounds of consultation. NBS has received the revised version from the UN Office of Legal Affairs and will go through procedures to obtain the approval for its signing as soon as possible." [42] We have not been able to verify the existence of such memorandum of

---

of the Secretariat's interpretation of the material scope of the protection offered by Art. II Section 4": Gian Luca Burci, "IV Immunities and Privileges, C Inviolability of Archives, Inviolability of Archives (Article II Section 4 General Convention)", *in* August Reinisch (ed.), *The Conventions on the Privileges and Immunities of the United Nations and its Specialized Agencies: A Commentary*, 2016, p. 161.

[39] Article II, section 3 of the Convention on the Privileges and Immunities of the United Nations.

[40] Report of the Joint Inspection Unit, Cybersecurity in the United Nations system organizations, 2021, JIU/REP/2021/3: "In other words, States, and in particular host countries, have a duty to protect organizations from hostile attacks, whether in the physical or in the digital sphere. This interpretation was confirmed to the Inspectors by the Office of Legal Affairs and settles the question of whether electronic data and digital assets are covered by existing legal provisions".

[41] I. Pingel, "Chapter 20: the privileges and immunities of the international organization", *in* E. Lagrange and J.-M. Sorel (eds.), *Traité de droit des organisations internationales*, *op. cit.*, pp. 645-646.

[42] https://unstats.un.org/bigdata/regional-hubs/china-concept-note.pdf

understanding (MoU). However, we can affirm that the legal value of an MoU does not equate the one of a proper headquarters agreement.

The data of the Organisation may be protected by the regime of immunities according to the legal qualification that will be given to them. Immunity may be absolute or only functional, *i.e.* limited to the protection of activities related to the performance of the organisation's functions. Practice has not settled the question, although the current trend is to question absolute immunity in the name of the protection of fundamental rights. Nevertheless, even if the principle of functional immunity were to be accepted, which is far from being the case, the data covered by the United Nations Big Data Programme, because it serves the objectives of the Organisation, would be protected in any case.

Furthermore, under the UN Charter (art. 103) as well as under EU law (art. 3, paragraph 5 and art. 21 of the Treaty on European Union, art. 351 of the Treaty of the Functioning of the European Union), the Member States of the European Union, as a member of the United Nations, are obliged to give precedence to their obligations under the Charter over any other international treaty obligations. This precedence of Charter obligations has been confirmed by the case law of the CJEU.[43]

The same reasoning applied to UN digital data with respect to EU law is equally applicable with respect to Chinese or any other law. No interference in the operations of the UN data is possible because of the immunity of its property and assets, the inviolability of its archives and documents and the inviolability of its premises. Several Chinese laws state that national authorities shall act "in accordance with law (…), shall preserve the lawful rights and interests of individuals and organisations" [44] and "may carry out foreign exchanges and

[43] *The Queen, ex parte Centro Com v. HM Treasury and Bank of England*, Case C-124/95, EU/C/1997/8, 14 January 1997, para. 57, 159, 288; Grand Chamber, *Yassin Abdullah Kadi and Al Barakaat International Foundation v. Council of the European Union and Commission of the European communities*, C-402/05 P and C-415/05 P, EU/C/2008/461, 3 September 2008; Grand Chamber, *Melli Bank plc v. Council of the European Union*, Case C-380/09 P, EU/C/2012/137, 13 March 2012, para 54.

[44] National Intelligence Law, Art. 8. See also, 2015 National Security Law, Art. 7 and 43.

cooperation."[45] It is also foreseen that organisations that are victims of abuse of authority or unlawful activity of state organs can file complaint appeals or reports.[46]

It should be noted that although espionage in itself is lawful under international law, it is nevertheless possible to identify activities that can be qualified as unlawful. This is the case, for example, of an action consisting in the unauthorized collection of data from an international organisation enjoying immunity. The unlawful act is then the violation of the immunity of the targeted organisation. If this act is committed by a State, the international organization may seek the international responsibility of the State. It could then adopt sanctions against it. However, such a hypothesis remains unlikely, especially for cases of espionage. Instead, the organization will certainly resort to official private or public protests (naming and shaming).

3. The data protection regime at the United Nations

The protection of human rights is one of the purposes of the United Nations along with the maintenance of international peace and security, the rule of law and development.[47] The General Assembly has also been able to recall the applicability of international human rights law in the digital sphere.[48] International human rights law allows for the protection of digital data, but beyond these general rules, the United Nations has more specific and internal rules of law.

The UN system has produced a set of internal rules and policies relating to data protection "concerning, among others, their respective staff and other personnel (...), vulnerable populations (such as refugees and migrants), vendors and other entities registered in the United Nations Global Market place, delegates and conference attendees, as well as

[45] National Intelligence Law, Art. 13. See also, 2016 Cybersecurity Law, Art. 7 and 2021 Data Security Law, Art. 11.

[46] See 2015 National Security Law, Art. 43 and 82; National Intelligence Law, Art. 19 and 31.

[47] Charter of the United Nations, preamble.

[48] GA resolution 68/167, *The right of privacy in the digital age,* 18 December 2013. See also GA resolution 44/132, *Guidelines for the Regulation of Computerized Personal Data Files*, 5 December 1989; GA resolution 45/95, *Guidelines for the Regulation of Computerized Personal Data Files*, 14 December 1990.

individuals included in the UN Security Council Consolidated Sanctions List of Those suspected or of involved in terrorism or the financial support thereof."[49].

The legal framework applicable to the processing of data by the United Nations includes

- Guidelines for the Regulation of Computerized Personal Data Files, adopted on 14 December 1990:[50] these Guidelines list guiding principles applicable, including to data processing by international organizations;[51]
- Personal Data Protection and Privacy Principles, adopted by the UN High-Level Committee on Management on 11 October 2018.

These are general principles that are not very precise; for example, no definition of personal data is given. Ten principles that should guide the processing of personal data by the organisations of the United Nations system are cited: fair and legitimate processing, purpose specification, proportionality and necessity, retention, accuracy, confidentiality, security, transparency, transfers, accountability. These principles are very similar to those that can be found in the GDPR or the PIPL and are part of what can be called today the common law of personal data protection. However, their affirmation in law is not sufficient. In order to be

[49] Letter from M. de Serpa Soares to A. Jelinek, 14 May 2020, 28 p., §5 and note 11: General policies concerning data protection are included in ST/SGB/2007/6, Information sensitivity, classification and handling, and ST/SGB/2007/5, Record-keeping and the management of United Nations archives. In addition, specific data protection rules are included, inter alia, in: ST/SGB/103/Rev.1, Rules Governing Compensation to Members of Commissions, Committees or Similar Bodies in the Event of Death, Injury or Illness Attributable to Service with the United Nations; ST/SGB/2003/18, Policy on HIV/AIDS in the workplace; ST/SGB/2006/6, Financial disclosure and declaration of interest statements; ST/SGB/2006/7, Records of the Serious Crimes Unit of the Office of the Prosecutor General of Timor-Leste; ST/SBG/2009/12, Records and archives of the United Nations Monitoring, Verification and Inspection Commission; ST/SGB/2010/3, Organizations and terms of reference of the Office of Administration of Justice; ST/SGB/2012/3, International Criminal Tribunals: information sensitivity, classification, handling and access; ST/SGB/2014/3, Employment and accessibility for staff members with disabilities in the UN Secretariat; ST/SGB/2016/7, Terms of reference for the Office of the UN Ombudsman and Mediation Services; ST/SGB/2016/11, Organization of the Office of Information and Communications Technology; and ST/SGB/2018/1, Staff Regulations and Rules, Appendix D. Several Administrative Instructions are also relevant to data protection, including ST/AI/2010/2, Request for rectification of date of birth or of other personal data, and ST/AI/341, Confidentiality of mailing lists and registers.

[50] GA Resolution 45/95, 14 December 1990.

[51] Commission on Human Rights, *Revised version of the guidelines for the regulation of computerized personal data files prepared by Mr. Louis Joinet*, Special Rapporteur, E/CN.4/1990/72, 20 February 1990.

able to assess the degree of protection of these data, it is also necessary to know how they are interpreted. Thus, in one of the letters exchanged with the Chair of the European Data Protection Board, the Under-Secretary-General for Legal Affairs and the United Nations Legal Counsel seemed to put forward the idea of a specific purpose for data processing by the United Nations, based on the "public interest."[52] This approach to data protection might appear to be more liberal than that required by the GDPR, even if public interest is an exception to certain data processing obligations under EU law.

The UN also has regulations for more specific areas, as in the case of data and the Big Data and SDGs programme.[53] Principle 6 states: "*Individual data collected by statistical agencies for statistical compilation, whether they refer to natural or legal persons, are to be strictly confidential and used exclusively for statistical purposes.*" These rules aim to implement the general principles set out above in a more precise manner.

Finally, other organisations of the United Nations system have a more advanced legal framework for the protection of personal data. Examples include the International Organisation for Migration[54] and the UNHCR[55] .

Both Chinese and European law provide for their application to legal persons, as data controllers. However, the status of international organisations, based on the international law of immunities, prevents in principle any application of this law to international organisations: United Nations and specialised agencies. This has two consequences. Firstly, if a State were to access an international organisation's data without its consent, it could thus certainly be held responsible. Secondly, it becomes necessary to refer to the internal law of the organisation in order to know the rules applicable to data protection. Although the principles and guidelines laid down by the United Nations are in line with the common principles of data

[52] Letter from Mr. Miguel de Serpa Soares, Under-Secretary-General for Legal Affairs and United Nations Legal Counsel, to Ms. Andrea Jelinek, Chair European Data Protection Board, RE: Impact of the European Union's Data Protection Regulations on the Activities of UN System Organizations, 14 May 2020, para 29.

[53] Fundamental Principles of Official Statistics, A/RES/68/261.

[54] Document IN/138, IOM Data Protection Principles, 2009; Policy on Migration Data Governance (Instruction IN/253) (Geneva, 2017); IOM Data Protection Manual, 2010; IOM Migration Data Strategy: Informing Policies and Actions on Migration, Mobility and Travel 2020 - 2025: Evidence on how IOM handles data.

[55] Policy on the Protection of Personal Data of Persons of Concern to UNHCR, (2015).

protection, their general wording does not seem to offer protection equivalent to that offered by European Union law, for example. The Chinese authorities might consider the same to be true with regard to the compatibility of UN law with Chinese data protection law. Exchanges of letters between the UN and the EU on the subject show the harmonisation efforts underway. If the United Nations wishes to preserve its status, it seems necessary to clarify its data protection rules, especially if the Organisation intends to embark on its digital transformation. There are many different data protection regimes.

Part 3: Specific Data Protection Regimes for Each Type of Data

Despite its immunities, the UN should continue its efforts to better protect its data. These efforts are of two kinds. Firstly, because of the diversity of data and its multiple origins, more and more European and Chinese laws are likely to seek to apply to UN data. The UN should therefore seek to develop a more comprehensive and protective data regime. Secondly, even though UN data is immune, several elements must be taken into account to secure data in the cloud, including when drafting the contract between the UN and the service provider.

1. The diversity of data from international organisations

International organisations have to process a multitude of data (see *above*, data relating to the SDGs). Each type of data requires a legal qualification (existing or not) and the application of a specific legal regime.

Some examples are given below:

- Data relating to staff (officials, agents) likely to be contained in employment contracts and all acts relating to staff management may contain personal data or even sensitive data, requiring special legal protection;
- The factual data on which the organisation's activities are based: data produced by the Member States, produced and processed by the UN bodies and agencies, which can be the subject of statistics;
- Documents relating to the functioning of the organisation may be internal: intended solely for their agents and bodies: memos, directives; linked to the organisation's service providers and partners: contracts, agreements. These documents may contain personal or non-personal data, classified or not, and may or may not be part of a policy of transparency of the organisation's activities and consequently of *open data*;
- Documents relating to the functioning of the organisation with an external scope: resolutions, declarations, *communiqués*, etc. These documents are usually published on the organisation's institutional website and are covered by *open data*.
- Documents relating to the organisation's operational activities include agreements with the host state, contracts with local contractors and subcontractors, agreements

with other international organisations, partnerships with private actors. They also include factual, personal and non-personal, sensitive and non-sensitive data.

- Data exchanged between UN agencies can also be mentioned. It is partly covered by the UN Big Data programme and may be subject to a protection regime and the legal regime for data transfer when exchanged in the context of transborder flows.

A study on the protection of data of international organisations requires a clear and precise identification of the data in order to qualify them. One piece of data may be subject to several legal qualifications and call for the application of several legal regimes.

Example: in the context of an international administration operation, the UN may collect data on individuals, which may be qualified as personal data, or even sensitive data, and could be transferred to other UN agencies or local institutional partners cooperating in the implementation of this operation. The location of the operation and the actors involved in the transfer of these data will also determine the applicable law. In the case of non-sensitive personal data collected without involving a European actor, compliance with international human rights law would be necessary: Art. 12 Universal Declaration of Human Rights, Art. 17 Covenant on Civil and Political Rights, provided that the State on whose territory the controller is located is a party to the Covenant. If the data processing involves a European actor (controller or processor), who transfers the data to the organisation, Article 44 GDPR is likely to apply: "*Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an* international organisation *shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined*." This is one of the points of contention between the EU and the UN.

2. The diversity of legal regimes for data protection

While the EU GDPR is relatively well known, EU law on data regulation is broader. In February 2020, the European Commission presented a data strategy which aims to develop a single market for data, facilitating the responsible access, sharing and re-use of such data, while respecting EU values and in particular the protection of personal data. This strategy

includes two proposed regulations: the Data Governance Act (DGA) and the European Data Act.

- The Data Governance Act was adopted in May 2022 and will be applicable in September 2023. It aims to encourage the sharing of personal and non-personal data by setting up intermediation structures. These may be digital platforms allowing the sharing or control of data by companies and individuals. The DGA provides for guidance and technical and legal assistance to facilitate the re-use of certain categories of protected public sector data as well as certifications for data intermediation service providers.
- The Data Act was introduced on 23 February 2022 and aims to ensure a better distribution of the value derived from the use of personal and non-personal data between the actors of the data economy. It aims to facilitate the sharing of data between companies (B2B) and with the consumer (B2C), to allow the use of data held by companies, to facilitate the change of data processing service provider, to provide for the development of interoperability standards for data, to put in place safeguards against unlawful access by third country governments to non-personal data in the cloud.

These proposed regulations have been the subject of joint opinions by the EDPB and the European Data Protection Supervisor (EDPS),[56] which draw attention to the risks of infringement of the fundamental rights of data subjects, fragmentation of supervision and difficulties of implementation, and stress the need to harmonise future legislation with personal data protection law. These alerts highlight the existing points of vigilance with regard to new data regulations and confirm the need for the UN to strengthen its normative framework in this respect.

[56] EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European Data governance (Data Governance Act), 11 March 2021; EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act). See also EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021.

3. Data protection in the context of cross-border data transfer

According to the GDPR, data transfers outside the EU may be based on:

- An adequacy decision by the European Commission concerning the countries with an adequate level of protection.[57] This is an examination of all the legislation in force in a State, on a territory or applicable to one or more specific sectors within that State.[58]
- In the absence of an adequacy decision, a controller or processor shall provide appropriate safeguards,[59] which may be provided for by:
    - "A legally binding and enforceable instrument between public authorities or bodies ;
    - Binding corporate rules in accordance with Article 47;
    - Standard data protection clauses adopted by the Commission in accordance ith the examination procedure referred to in Article 93(2);
    - Standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
    - An approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
    - An approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights."

According to Article 38 of the Chinese PIPL,

[57] https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

[58] Art. 45, GDPR.

[59] Art. 46, GDPR.

> "Where a personal information processor needs to provide personal information outside the territory of the People's Republic of China due to business or other needs, it shall meet any of the following conditions:
>
> (I) where it has passed the security assessment organized by the State cyberspace administration in accordance with Article 40 hereof;
>
> (II) where it has been certified by a specialized in accordance with the provisions of the State cyberspace administration in respect of the protection of personal information;
>
> (III) where it has concluded a contract with an overseas recipient according to the standard contract formulated by the state cyberspace administration, specifying the rights and obligations of both parties; or
>
> (IV) where it has satisfied other conditions prescribed by laws, administrative regulations, or the State cyberspace administration.
>
> Where the international treaties and agreements that the People's Republic of China has concluded or participated in have provisions on the conditions for providing personal information outside the territory of the People's Republic of China, such provisions may be complied with.
>
> Personal information processors shall take necessary measures to ensure that the processing of personal information by overseas recipients meets the personal information protection standards stipulated in this law".

Articles 39 to 43 of the PIPL protect both the rights of data subjects and national security, under the control of the Chinese authorities. The latter can include offending organisations "in the list of restricted or prohibited provision of personal information (...) and take measures such as restricting or prohibiting the provision of personal information to such overseas organisation or individual" (Article 42, PIPL). Finally, by virtue of the principle of reciprocity, the Chinese authorities reserve the right to adopt "discriminatory prohibitive, restrictive or other similar measures" against States that have done the same to them (Article 43, PIPL).

Whether it is EU law or Chinese law, the regulation of international data transfers is a means of controlling such data and thereby extending the application of its standards of protection (of the data subject's rights or of national security) beyond its territory. Such transfers may justify the extra-territorial application of data protection law. This is why it is important to anticipate these transfers, to adapt data protection standards or to offer appropriate safeguards that can satisfy all stakeholders.

4. Protection of data stored in the cloud

The United Nations Joint Inspection Unit had warned about the risks that external hosting services could pose: "The loss of extraterritoriality status of United Nations system organisations using an external hosting service is also a very serious risk. It can lead to a loss of confidentiality of data since, in some Member States, authorities have the right to demand access to data stored on the server of an external service provider that is not part of the United Nations and is not located on the premises of a United Nations organisation."[60]

Even though UN data is immune, there are a number of elements that need to be taken into account when drafting the contract for the provision of cloud computing services:[61]

Information on processing: compliance with data protection principles, systems for reporting complaints and security breaches, means of processing, recipient of data, subcontracting, existence of simple procedures for respecting the rights of data subjects in relation to their data;

The guarantees implemented by the service provider: limited and reasonable data retention period with regard to the purposes for which the data were collected; destruction and/or return of data at the end of the service or in the event of early termination of the contract in a structured and commonly used format, duty to cooperate with the competent data protection authorities;

Location and transfers: clear and exhaustive indication of the countries hosting the service provider's data centres where the data will be processed; assurance of adequate protection abroad (in particular thanks to standard contractual clauses or binding corporate rules "BCR"); possibility of limiting data transfers only to certain countries recognised as providing an adequate level of protection; information to the customer in the event of a request from a foreign administrative or judicial authority;

---

[60] AGNU, *Rapport du Corps commun d'inspection sur les sercvices d'hébergement information auxquels font appel les organismes des Nations unies (JIU/RES/2008/5)*, 7 octobre 2009, A/64/96, p. 11, para. 41 (our translation).

[61] For example, see CNIL, Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing, p. 8-9.

Security and confidentiality: indication of the provider's data obligations, security policy and minimum security measures; certifications; reversibility/portability; traceability; service continuity, backups and integrity; Service Level Agreements.

International organisations mobilise a multitude of data, which require different legal qualifications and regimes. Even if these data could be protected by the regime of immunity, it seems useful for the Organisation to take all the legal and security precautions necessary to protect itself from possible intrusions by external entities into its data. These precautions consist, on the one hand, of a more detailed identification of the data to be protected and, on the other hand, of the adoption of a more precise legal framework, whether it be the organisation's internal rules, the agreements to be concluded with the host States or the contracts concluded with the digital service providers.

Conclusion and recommendations:

This study has shown that the storage of UN data in China or by Chinese actors does not impede the application of UN privileges and immunities. This results in the protection of Dutch and EU citizens' data vis-à-vis the Chinese State as soon as the data is transferred to the UN. The transfer of data to the UN leads to the application of UN domestic law. However, UN data law is not well developed and does not appear to be as protective as EU law. Further steps could be taken by the UN to better protect data. The development of a more thorough normative framework for data protection within the UN should be therefore supported, as well as any technical or contractual measures that can better ensure the effectiveness of UN privileges and immunities.

Recommendations:

1. Adapt contracts with cloud service providers to the specificities of UN data. In particular, ensure that there are specific security obligations for the hosting provider to ensure the physical and IT security of UN data.
2. Encourage the conclusion of an agreement between China and the UN on the Regional Centre for the UN Global Platform or, if it already exists, ensure the recognition of the immunities of the stored data and the inviolability of this Regional Centre;
3. Encourage the development of a more precise data protection framework within the United Nations in order to ensure a level of protection equivalent to other data protection systems, notably European, and thus facilitate the international transfer of data;
4. Continue the discussions between the EU and the UN on data transfer and anticipate the normative developments resulting from the European Data Strategy, in particular the DGA and the Data Act.