Data as business value: Maximizing data assets through contracts

Mariana Chapei
Foreign Lead Lawyer

When discussing data with companies, it's common to hear "this is not an issue, we don't collect personal data." When asking further questions, we see that the company processes IP addresses, or geolocation information, and others that may, indeed be considered personal data depending on the context[1]. Furthermore, even if the company indeed does not collect personally identifiable data, there are very few enterprises in the world that do not rely on data generated and process by its operations, its clients, or from other sources to add value to its business.

In fact, in today's world ***data is value***. Data is probably the most valuable asset of many companies.

Data can provide operations, marketing, and management insights for businesses. The correct use of data collected by the company itself or received through collaborations or partnerships can boost revenue. Those who can learn how to protect it and how to exploit it in the best way will grow sustainably. Yet, in most cases, when companies negotiating agreements, it is common to pass through data provisions and rely on boiler plates not specific to their business model.

To maximize the value of the business through the use, sharing, or receipt of data, companies' representatives should carefully assess how the processing of data aligns with their business strategy and evaluate each circumstance and new deal regarding such data to properly address them in agreements.

Amongst several topics that require attention, which shall be defined from case to case, some issues repeatedly call for consideration in most every deals.

What is the data?

Generally, data is information. Parties in any commercial relationship continuously share information. Not all information is valuable and needs to be protected. The parties should ponder and discuss about which data is relevant enough to each of them that needs to be safeguarded by creating rights and obligations between them. For example, in some cases, the data may be personally identifiable data, in other cases, business data such as delivery routes or inventory control.

It may seem obvious to state that the parties should define the data, however not uncommonly there are discussions regarding what information is object of increased commitments. On one side, the party receiving the data wants to narrow the scope of the obligations regarding use limitations, deletion, security and safety of data received during the business relationship to only a specific set of data so it can be free to use certain information obtained during the performance of the contract to its own business purposes. On the other, the party that shares its data (for any reason, including for using software provided by the receiving party) seeks to ensure that the receiving party properly protects and does not make unwanted use of information that is crucial to its business development.

In addition, different jurisdictions (e.g., Europe and United States), and sometimes different regulations in the same jurisdiction[1], have distinct definitions on what data is. These variations in meaning may cause each party to understand data in a unique matter, showing the importance of a discussion regarding the data subject of the restrictions in the agreement.

Who is the owner of the data?

Once a party defines what data or data set is relevant to its business, the question becomes how to ensure that it can use the data as it wishes. In some situations, the data is created by the performance of the agreement and be difficult to interpret who has the right to control its use. For example, a truck freight company establishes a partnership with a provider that will optimize the delivery routes and, for that, installs geolocation devices in the trucks. The routes and location data of the trucks are then saved in a third party cloud provider. Who can use, download, sell, transfer, share, process, analyze or decide how the data can be used? The freight company, the provider, the owner of the geolocation devices, the cloud provider?

In most cases, the parties should establish clearly that certain data belongs to a party or another and not believe that it is "implied" that it will be owned by this or that party. The "ownership of the data" is a common but mostly overlooked clause. If there is sharing of data sets by both parties and/or separate data sets that arise from the performance of the contract, each data set may be owned by a different party and that should be clearly stated in the agreement.

On another note, since there is no law that states or refers to ownership of data[2] and traditional concepts of ownership may not apply to data (it is not a physical good) and intellectual property regulations also do not cover sets of data (as data usually lacks signs of originality that creates intellectual property rights)[3], merely stating that data is owned by a party may not be sufficient for the performance of the contract or its protection. In fact, many different people may access the same data simultaneously and still benefit from the same data.

Furthermore, the service provider may need to process the data to provide the services, and then it becomes necessary to delineate what each party can do with the data under discussion to avoid misuse or misappropriation.

The parties must think ahead and consider possible issues that can be created. In fact, even if most of the processing is usually done by computer programs, however, there may be the case that a person needs to access raw data to troubleshoot an issue. Defining the actions a party can do with the data of the other party becomes an essential part of the discussion.

What happens to the data at the end of the contract?

Business relationships end. They end for many reasons, being because the service was provided or the product was delivered, or due to misunderstandings between the parties, or even breach, or simply for non-renewal. Company representatives must understand the data that is being shared or processed under that business engagement and foresee how it should be handled once the business relationship ends. And have this handling agreed as a right and obligation under the agreement to avoid surprises in the future.

As discussed previously, each case is unique and requires proper consideration to outline the best manner to manage transition. For example, in some cases, one of the parties has its data in the other party servers or systems and will need to withdraw it. What is the intended method of data retrieval? In which format? What is the period of the delivery of the data? It's not difficult to understand how contentious this can be if not defined previously, and these are just preliminary questions.

On another note, the party receiving the data may have legitimate reasons to keep the data in one manner or another, such in the cases when data is needed to improve the services and products, and machine learning training[4]. Or part of the services is to deliver certain aggregated data collected from customers. If allowed, how the data is to be kept (e.g., raw, pseudonymized, anonymized, aggregated, etc.)? What are the permitted uses or the allowed processing, if any, of the data? How can it be verified? All such items, and more, should be discussed as soon as possible and not at the end of the commercial relationship.

Is there anything else the parties should think about?

Yes, certainly. As indicated above, when a business transaction involves the transfer of data from one party to the other, or the creation or gathering of new data, regardless of whether sharing the data is the main object of the transaction or it is ancillary to it, each party must review, assess, and look into the future to properly address its concerns and secure the value of their own data.

Apart from the topics listed above, many other issues present themselves and need to be addressed. Some examples are the right to audit the data and the use of it by the other party, the quality and accuracy of the data being shared, whether the data should be considered confidential information (and thus, creating duplicated obligations under the same object or being possible to be disclosed if public information as provided in the confidentiality clause), compliance with applicable law (and whether it is possible to foresee all applicable law to the case in hand), and not to mention all the different issues that comes from use of data in artificial intelligence[5], and especially generative artificial intelligence and how data can be used in outputs. Moreover,

computer systems which process data are considered a product under the new EU Product Liability Directive, that may lead to compensation for damages.

In the absence of a check list that can be used for all cases, there is guidance and support that can be provided to help to ensure that a party obtains the best value out of the deal and secures its business assets.

[1] In the European Union, for example, the Data Act defines data as " any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording," while the GDPR only defines "personal data" and "data concerning health" and the Artificial Intelligence Act defines what "training data," "validation data," "testing data," and more.
[2] The EU Data Act focuses on data holders (not data owners) and regulates accesses and uses that third parties may have on the data held by such holder.
[3] In the EU, the Database Directive (Directive 96/9/EC) regulates legal protections for certain databases, however it "shall not extend to their contents and shall be without prejudice to any rights subsisting in those contents themselves."
[4] Use of data for machine learning, large language models, and other artificial intelligence related systems were purposefully left outside of the scope of this newsletter due to its complexity, which demands its own separate review.
[5] The parties must consider the new regulations, not only in the Europe Union (the EU AI Act and the proposed Artificial Intelligence Liability Directive), but in other countries and jurisdictions (e.g., the United Kingdom has issued a public consultation on proposals to introduce an exception to copyright law for AI training for commercial purposes).

Services	Immaterialrett og teknologi
Sectors	Technology