Data Management Guide for Small Business

An introduction to data management for micro-, small- and medium-sized enterprises

universität wien

ICC

Please cite as:

ICC (2023), *Data Management Guide for Small Business: An introduction to data management for micro-, small- and medium-sized enterprises*, https://iccwbo.org/publication/data-managment-guide-for-small-business/

© ICC 2023

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Please note that this outline cannot replace the consultation of legal professionals. It does not take into account the applicable national or regional/supranational law. The authors cannot assume any liability/responsibility regarding this outline.

Table of Contents

Introduction

Data has become an essential part of business life, driving global trade and productivity across all sectors of the economy. Enterprises of all sizes, sectors and regions increasingly depend on data to conduct business and create value for their organisation, employees and local communities. Ensuring that all businesses can implement good data management practices will enable greater compliance with evolving regulatory environments and empower businesses to better use and more readily share data to uncover new sources of innovation and growth.

However, not all businesses are equally equipped to seize the many new opportunities that data is helping unlock. Micro-, small- and medium-sized enterprises (MSMEs) often require specific guidance on how to manage and leverage data to become truly data-driven organisations and to seize new growth opportunities.

This data management guide for small business, developed jointly by the International Chamber of Commerce (ICC) and by a team from the University of Vienna involved in the preparation of the [ALI-ELI Principles for a Data Economy](#), aims to fill that gap by introducing businesses to key concepts of the data economy and providing a concrete methodology and best practices to properly leverage data and play a more active role in the data economy. Building on the ALI-ELI Principles and on expert input from members of ICC, this document will help MSMEs better navigate their data ecosystem and leverage data flows within it.

While this guide is not meant to replace consultations with legal professionals when necessary or appropriate, in particular when dealing with personal data or data that is protected by intellectual property (IP) rights, it can provide businesses with a useful introduction to data management and point out situations where specific regimes can come into play and where businesses might want to consult legal professionals familiar with the applicable regimes.

1. Why is data important to your business?

In recent years, there has been enormous progress in expanding connectivity and democratising the use of digital technologies. Data sits at the centre of this transformation. When properly harnessed, data can enhance business processes and customer service, help create more tailored products and services and create new revenue streams. Overall, data helps businesses make better informed decisions thereby ensuring a more effective allocation of resources at every step of business activity and operations.

Businesses can seek to **generate value** from data in six key areas:

🔍 Identifying customer experience issues	**Why is data important?**	Monetising data & creating sources of income 🚀
📊 Improving products and services		Identifying problems in internal processes 🧩
💡 Developing new innovative services		More targeted and efficient advertising & sales 🎯

Experiences of ICC Small Business Champions, illustrating how MSMEs are generating value from data, are available in Annex I of this document.

2. How should you manage the data you control?

All organisations, including small businesses, require a data governance regime – an overall system of strategic direction and oversight over all data management activities. Data governance ensures that data is adequately managed, used and protected across the whole organisation. This section aims to introduce MSMEs to good data governance practices and help them better understand what should be considered when dealing with data under their control.

Implement tailored data management practices

Data management is often said to have the goal of getting "a single version of the truth". This refers to the value of having one shared source or master copy of the data about the most important business entities, such as customers and vendors. Problems arise when there are multiple inconsistent versions of data. This can cause confusion and create flawed conclusions from the data as well as other mistakes. Proper data management includes having a shared and definitive copy of data with agreement on its structure, what attributes are in the records, how fields are formatted, what are legitimate entries and how the data must be captured and checked.

Data quality is vital for business operations and decisions. Data quality means the degree to which data serves its purpose in a particular context. Data must be

- Accurate – data is exact, free of errors and reliable.
- Complete – data represents what needs to be known.
- Relevant – data fits the intended purpose.
- Timely – data was captured at the right time and kept up to date.
- Accessible – data is captured in productive formats that people and applications can easily access.

Data quality hinges primarily on file naming and metadata conventions. Organisations must create a file system that is user friendly, descriptive and standardised to allow all potential users to search and discover datasets. Key to this is metadata.

Metadata holds descriptive information about the organisation's data, which contains information about the data's content, structure and access permissions. For example, metadata can include information about the data source, author and date of creation. This information ensures that all stakeholders within the organisation have a common understanding of the data lineage from its origin to its destination. Without proper file naming and metadata conventions, an organisation will struggle to find specific information and will be unable to use its data effectively.

Implement adequate data lifecycle management practices

Organisations must also consider when to retain and delete data. This is part of data lifecycle management which looks at the evolution of data from creation and initial storage to when it becomes obsolete and is deleted. While organisations should aim to store as much data as possible, limited storage capacity and associated costs often mean that businesses must decide which data should be stored for extended periods of time and which data should be deleted.

Each business will have different priorities, but as a general rule, businesses should retain data that is (1) associated with compliance or regulatory obligations, (2) associated with customers, suppliers and business partners and (3) necessary for everyday business operations. You may wish to store further data for the purpose of (4) value creation, as far as this is possible under applicable law, in particular data protection law.

Data that is retained must be stored in a stable environment and properly maintained to ensure its integrity, security and protection. While it is stored, the data is usually processed and transformed, which means that special attention must be paid to ensuring its continued reliability and recoverability. Once data assets are no longer necessary for the organisation's everyday operations and workflows, it must be archived to a secure storage system. Crucially, all data that may be necessary from a compliance or reporting perspective must be securely archived. When data assets become finally obsolete, they can be permanently deleted, provided this is done in a secure way and does not contravene local data protection requirements.

Build a data-driven organisation

Creating value from data requires specific human resources, tailored technical solutions and a business culture in which everyone understands the value of data. Becoming a data-driven organisation requires a cultural shift across the whole business. This transition should aim at building a framework that empowers all employees to leverage data assets in a collaborative way to advance individual and team objectives. Employees should put data at the heart of their activities and use data to initiate and implement projects and initiatives. Therefore, the organisation should aim to consolidate data assets in a single repository and minimise barriers to access whenever possible (e.g. in line with data protection regulations).

Transitioning to a data-driven organisation may also require investments in technological solutions and tools that are properly tailored to the needs of a business organisation. Data management tools can provide myriad services and solutions such as archiving, recovery, search and analytics,

which can help manage data assets effectively and securely. These tools fall into the following categories:

- Cloud data management tools, which manage data across cloud platforms, in combination or instead of on-premises storage.
- Data integration tools like ETL (Extract/Transform/Load) or ELT (Extract/Load/Transform), which combine data from multiple data sources into a single, consistent data repository.
- Data transformation tools, which convert data from one format to the required format of a destination system.
- Master data management tools, which help ensure accurate, up-to-date data.
- Data analytics and visualisation tools, which help draw useful insights from your data assets.

In addition, staff with specialised skills can go a long way in helping an organisation become more data-driven. These specialised profiles include:

- Data analysts and scientists, who specialise in analysing data sets to advance business objectives.
- Data engineers, who ensure that data is collected, curated and made available within the organisation.
- Data platform administrators, who manage the data infrastructure, implement access control and security policies for the organisation.
- Data compliance officers, who ensure that the data is collected and utilised in accordance with local regulatory requirements.

Ensure strong data security and privacy

Data security and data privacy/protection are separate but similar and essential concepts. Data security entails putting provisions in place to ensure data is not subject to unauthorised access by malicious actors. Data that is sensitive, important or proprietary needs to be protected. This means that businesses must systematically identify and classify sensitive data, monitor its access, implement multi-factor authentication to access sensitive data and use endpoint security systems (e.g. antivirus software, antispyware, firewalls etc.). Other best practices for effectively securing data include ensuring passwords are secure, avoiding unsecure networks, ensuring devices are physically safe and systematic compliance with clearly documented company rules. Furthermore, it is essential that all employees are properly trained and kept up-to-date on new protocols and company rules.

Data privacy and protection is intrinsically linked to third party rights and protective regimes, which are mostly determined by national (or regional) law. Data privacy law only applies to personal data or personally identifiable information, which is often defined as information that allows for the identification of an individual or can be linked to an individual, like their name, address or personal preference. Data that is non-personal is mostly subject to less protective regimes, which means it can be shared more easily. Data protection regimes usually also apply to pseudonymised data, where the original data set is replaced with a pseudonym or alias. When sharing certain data, businesses must ensure they comply with all requirements under these

protective regimes, e.g. by obtaining consent from the third party. It is critical to handle such data with extreme care, as the individuals whose data you are holding are counting on your business to comply with expected standards, which might vary in different regions.

Case study on personal data protection

Your business is an online shop that gathers contact information from customers. Even storing the data would make you a data holder (controller) under most data protection regimes. If you agreed with your customer to ship a product to their home, you will most likely be allowed to use the address they provided for the shipping process and provide them to a parcel service. However, if you would like to sell the data to another business (e.g. for marketing purposes), you will most likely have to ask for your customers' consent to do so. When buying customer data from another company, also make sure all processing steps are justified, most likely by the customers' consent. In any case, make sure to comply with local data protection regimes or approach your regional chamber of commerce for help.

Other third-party rights can be drawn from IP law, for example, where a third party has a copyright regarding the data in question (e.g. on text or pictures or even databases). Businesses also have to comply with third-party rights under national and/or regional IP regimes.

Case study on IP protection

For the purposes of training artificial intelligence (AI), your business requires large amounts of text to carry out text and data mining. Another business holds the copyright in suitable text data, which you would like to use and is accessible online. Before using this copyright-protected material, make sure to receive a license from the holder of the copyright or check local copyright law to verify whether an exception applies in your case (e.g. for training AI for scientific purposes). The same holds true for using picture or audio material on your businesses' website.

3. Where do you sit in the data economy?

As a business, it is important to first understand where you sit in the wider data ecosystem to take appropriate steps for your organisation and engage accordingly with other stakeholders in this data ecosystem. Businesses take on different roles in the data economy, depending on their involvement with certain data. The diagram below highlights key stakeholders in the data ecosystem and associated data flows between them.
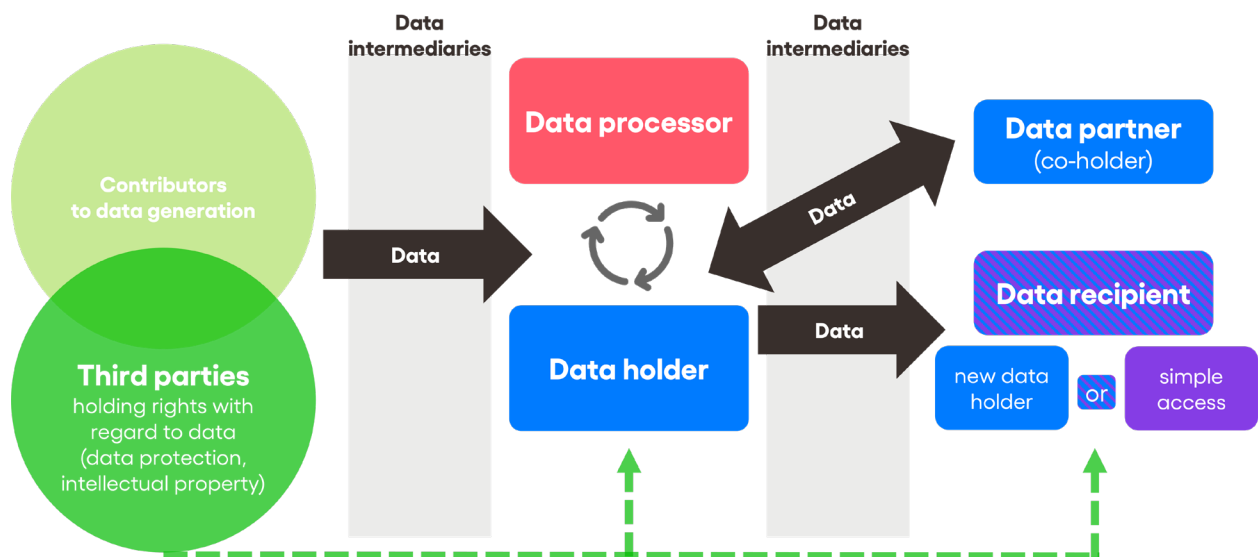
'Players and Relations in the Data Economy' © Christiane Wendehorst, graphic design by ICC

Data holders (controllers) are the central players in all data ecosystems. They have access to data and decide how to use and process this data. Two or more data holders can cooperate and pool their data – this makes them data partners (co-data-holders).

- Are you in a position where you can decide what to do with the data and how to do it (e.g. store the data on a cloud server, organise the data in a filing system, filter customer information from the data, link different data sets or even delete data? If your answer is 'yes', you are probably a data holder/controller.
- Do you hold such data together with another company (e.g. shared customer database)? Can you both decide the purposes and means of data processing (e.g. both partners use a joint booking platform for marketing their services)? Then you are probably a co-data-holder.

Data processors, however, do not have full control over the purposes and means of data processing. They are (external) service providers that process data on a data holder's behalf.

- Does your business carry out data processing activities for other businesses (like storing/organising employee data from another company in your own IT system or creating advertisements from data provided by the other business through your personalisation software)? Is the purpose of the data processing activity and the means chosen to process it specified by another business? Then you probably are a data processor.

A data holder can supply data to data recipients. The holder can either fully transfer the data to a new data holder or only provide simple access to the recipient.

- Have you received or bought data from a data holder (e.g. for marketing purposes, market research) or are you planning to do so? Have you been put in full control of data or at least been provided with access to data? This would make you a data recipient.

Parties can contribute to the generation of data in different ways, e.g. by being the subject of information recorded in the data or by operating a device that generates data.

- Does your business use connected products like smart vehicles/machines that generate data, which is stored and processed by another business? Does your business use online platforms to market products or services, providing data to the platform operator? In all these cases, you will likely have contributed to the generation of data and may have certain rights against the data holder.
- On the other hand, if your business holds data that has been co-generated through the contribution of others, such as the users of connected products, you may have to respect certain rights of parties that have contributed to the generation of data.

Parties may also have third-party rights against the data holder(s) with regard to the data (e.g. derived from data protection or IP).

- If you are a data holder or data recipient, do you handle data that is linked to any third parties (e.g. customer data, data about other businesses, IP-protected graphics for marketing purposes, etc.)? If yes, always make sure you do not infringe any third-party rights in handling the data.
- On the other hand, if you feel that another data holder is infringing your rights, such as by exploiting your trade secrets without your consent, you may wish to take action against the data holder.

Relationships between parties assuming any of the aforementioned roles may be greatly facilitated by data intermediaries.

- If you would like to share data you hold or generate with third parties in a reliable manner but do not have the resources to monitor what those third parties do with the data and whether or not they comply with conditions, you may consider using a data trust service.
- If you just want to monetise your data or if you are looking for particular data and do not readily know where you could get them, you may wish to use the services of a data marketplace.
- You may also decide to act as a data intermediary yourself, in particular where you have contacts both with parties holding or generating data and parties that are interested in data re-use.

Note: These roles are not mutually exclusive, and businesses often take on several roles in the context of their operations and business relationships.

4. What should you consider when sharing data or receiving data from other businesses?

Data can be shared between a data holder and a data recipient based on a data sharing agreement. When entering into such contracts, both the business sharing data (data holder) and the party receiving data (recipient) need to consider the special characteristics of data, as every data transaction is different. When sharing or receiving data, in any case make sure to check compliance with regimes that protect third-party rights (e.g. data protection or IP rights, also see chapter 3). When negotiating a data-sharing contract, a first strategic decision concerns the extent to which the data recipient can access the data:

✓ Full control or simple access?	• **Should recipients get full control of the data?**
	   ○ Recipients are allowed to download the data to their own servers.
	   ○ Recipients can integrate data in their own IT infrastructure and can decide how to use the data.
	
	• **Or should recipients only receive simple access to the data?**
	   ○ Recipients may access the data only on the data holder's IT infrastructure (*in situ* access).
	   ○ Holder can monitor the recipient's processing activities more easily.

There is a range of additional decisions that can be taken by the parties negotiating a data-sharing contract, e.g. regarding possible limitations on the use of data supplied and with respect to the quality and quantity of data that needs to be provided under the contract by the provider of the data:

✓ Limitations on use?	• **For which purposes may recipients use the data?**
	   ○ Recipients may use the data only for certain purposes mentioned in the agreement (like the development of a new product) <u>or</u>
	   ○ they are free to use the data for any (lawful) purpose.
	
	• **Are recipients entitled to pass data on to other businesses?**
	   ○ Recipients may not pass the data on to third parties <u>or</u>
	   ○ they may only share data with certain businesses and/or for certain purposes <u>or</u>
	   ○ they are free to share data with any third party.
	
	• **May recipients use derived data that they generate from processing the supplied data?**
	   ○ Parties can decide on similar conditions for and limitations of use of derived data as for the data initially supplied by the data holder.

✓ Properties of the data?	• **Which qualities of the data are required under the agreement and for how long should the data be provided? Which other obligations need to be fulfilled under the sharing agreement?**
	   ○ Recipients may require data that is fit for a certain data activity (e.g. data on consumer preferences for marketing purposes) <u>and/or</u>
	   ○ recipients may access data only occasionally <u>and/or</u>
	   ○ recipients may require real-time access to data <u>and/or</u>
	   ○ the data holder is required to provide additional support, e.g. by keeping the data up-to-date, solving technical issues

5. What should you consider when engaging in the co-generation of data?

Data can be generated by the contribution of multiple parties. Often MSMEs will generate such data without their knowledge and as a by-product of an economic activity (e.g. by using connected machines or Internet of things products). The holders of such data may deny or limit data access because it can have significant economic value. Denying or limiting access to a party that has contributed to the generation of data may be contrary to national or regional law, such as competition law or regulations specifically addressing mandatory data sharing between businesses. However, it may be advisable to negotiate appropriate data sharing regimes already upfront before entering into an arrangement. This is why MSMEs should be aware of certain scenarios in which limited or denied access to such co-generated data may negatively affect their business interests in the long run:

Scenario 1: Access to repair or maintenance data

Your business might use **connected machines** and might need data produced by the machine for its **repair or maintenance**, like performance data to detect the reason for a defect. However, the data holder might deny any access to repair or maintenance data. This prevents your business from having the machine repaired by an independent or in-house technician.

What can you do? Before concluding a contract on the purchase or lease of a connected machine, make sure to negotiate a clause on access to repair or maintenance data.

Scenario 2: Quality monitoring

When your business supplies, e.g. **parts for a machine** that is produced by another company, you may need access to the data generated by the final machine in order to evaluate whether the **final product is working** as intended. However, the data might be stored on the servers of the company that produces the final product.

What can you do? When negotiating a contract on the supply of machine parts, you might want to add a clause on access to data generated by the final machine.

Scenario 3: Developing an associated product

If your business wants to **develop new products** that are **associated to another product that generates data** (like software or apps for a connected machine), you will likely need access to data from other companies. For example, if your company wants to develop a predictive maintenance service for a connected machine, it requires access to data generated by these machines to find out its characteristics and lifespan.

What can you do? If you are planning to develop new products that require certain data, you are well-advised to negotiate data access rights (e.g. to data generated by connected machines) with the data holder.

Scenario 4: Switching an porting data

Data holders can sometimes **prevent your business from switching suppliers** by simply denying any access to the user-generated data after termination of a contract.

What can you do? When agreeing to a contract, make sure that your business will have rights to access all the data that is necessary to switch suppliers. You could also add a clause that obliges the data holder to transfer the data to a new supplier (data portability right) or to comply with obligations under voluntary Codes of Conduct (that deal with switching and porting of data).

Annex I: Experiences of ICC Small Business Champions

Below are examples of how MSMEs have used data to achieve success in customer experience, supply chain management, product and service development, internal processes and advertising.

- **Identifying customer experience issues** (Rohit Mehrotra, Managing Director, NMK Textile Mills India)

"*As a manufacturer and seller of consumer products, we pay a lot of attention to customer experience, particularly complaints and suggestions. We have a dedicated customer experience team which reviews each complaint/feedback/suggestion and buckets them into categories and then provides that data to various internal and external stakeholders (e.g. vendors/suppliers). With this data, we can identify customer experience issues, and working with our R&D and manufacturing team we are able to address these issues by making the necessary changes in the manufacturing process. This helps us continuously improve our product features and customer experience.*"

- **Improving supply chain management** (Jürgen Lindenberg, Co-Owner, Lindy Electronics)

"*As a leading importer and supplier of IT and AV connectivity products and solutions, data gathering and analysis is essential to optimise our supply chain. For example, we must closely align key imports from China, which require careful planning and bulk purchasing over several months, with customer requirements for next day deliveries. This requires careful planning and detailed data on product quantities, turnover, demand cycles and cost per product. In order to measure and weigh each one of these variables, you need full access to the data in your enterprise resource planning system, clever thinking and a dashboard that lets you play around with the data to make the right decisions. And, of course, this data must be treated with care and a clear and comprehensive data security strategy.*"

- **Developing and improving products and services** (Victor Dosoretz, Founder and CEO, Mantra Group)

"*As a leading cosmetics brand in South America reaching markets across the globe, our product offers and associated services have to continuously adapt to new customer requirements and expectations, both offline and online. With the right data, we can produce the right product and sell at the right price, at the right place. This can only be achieved by gathering data from different sources and effectively analysing it in light of the wider business strategy. This includes both internal data (sales history, customer data, etc.) and external data (e.g. social media data, search data etc.). At Mantra Beauty, product and service specs are evidence based, as is our customer segmentation. By using new sources of data, we were able to better segment our customer base and develop new products and communications strategies aligned with our key demographics.*"

- **Developing new innovative products and services (Pinaman Owusu, Founder and CEO of ADJOAA)**

"ADJOAA is an online marketplace that supports the development of clothes designers and brands from Africa. One of these brands, based in a peri-urban city in Ghana, had outgrown its domestic market and was looking to expand to other parts of the African continent. By working with ADJOAA, the brand was able to track monthly its business insights into source of traffic, average order value, gross merchandise volume as well as purchasing trends in new test markets and customer segments of interest. The data provided insight into sales, products and customers across the platform. For example, most of the customers on the platform were in their early 30s to mid 40s with disposable income. Among that cohort were new parents looking for unique and affordable products for their children. This intelligence enabled the company to diversify its offering to include products aimed at mums and children. Thanks to its access to more data and business insights, the company was able to make more informed decisions, along with being innovative as it expanded its reach to new markets."

- **Monetising data and creating sources of income** (Victoria Alonsoperez, Founder and CEO, Chipsafer)

"Thinking creatively about your customer data can help improve your business and create new revenue streams. At Chipsafer, we developed an 'Internet of Things' platform that gathers cattle tracking data with smart devices and then transforms that data into actionable insights that help our customers improve the efficiency of their operations. On a broader canvas, this same data can then also be used to generate value from other stakeholders in the supply chain. For example, farmers benefit from knowing the location of their herd in real time. This traceability data can then also be used to achieve transformative transparency across the whole meat supply chain, enabling suppliers to show their consumers the location and journey of their animals from farm to fork. Verifiable and transparent data builds confidence and integrity and reinforces value and customer loyalty. These same principles can be applied across many sectors."

- **Identifying problems in internal processes** (Josie Morris, Managing Director, WoolCool)

"Data isn't just about the external world or what you gather as a consumer-facing e-commerce brand. Data is a useful tool for all types of companies to use from internal sources to improve processes and efficiencies. Internal analytics is a great way to start your data management journey as it is something you have full control over and does not require a detailed understanding of complex data protection rules. As a leading sustainable packaging manufacturer, we have used the data from the analysis of time and motion study, combined with product dimensions to work out exactly how many team members we need for each product we produce. This has allowed us to increase our productivity levels and plan our schedule specific to each product line, meaning our costs are optimised, production is more consistent, and we are not over or under-staffed."

- **More targeted and efficient advertising and sales** (Anna Nordlander, Founder, Acnor AB)

"*Selling on a large platform, we have always had very little access to customer data. This has forced us to find ways to combine data from different sources to make sure our content was reflecting our customers' needs. We used a combination of data gained from product reviews, customer interactions and our advertising efforts to improve our products and product descriptions. That has been a crucial component of our continued success. When you use data and truly listen to your customers, you take away the guesswork. This is also true for advertising: for our business, it has been crucial to use data gained from different campaigns to continuously improve those campaigns and lower the cost of advertising by smarter targeting.*"

About the International Chamber of Commerce

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 130 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28   E icc@iccwbo.org
www.iccwbo.org   @iccwbo

About the University of Vienna

The University of Vienna is one of the oldest and largest universities in Europe. Around 9,900 employees work at 20 faculties and centers, including around 6,900 scientists. It is the largest research institution in Austria and the largest educational institution in Austria. The team involved in this project consists of Nina Hafner-Thomic, Sebastian Schwamberger and Yannic Duller. They carry out research in the field of law and digitalisation, in particular on topics like data protection and data law. If you would like to contact the team at the University of Vienna, please reach out to nina.thomic@univie.ac.at

universität wien

Universitätsring 1, 1010 Vienna, Austria
T +43 1 4277 0   E icc@iccwbo.org
www.univie.ac.at   @univienna