WHY DO WE TALK ABOUT THIS?

iBinder AB provides a cloud-based document management system on iBinder.com.
You as our customer can store and process a large amount of information when you use our service by uploading documents, providing descriptions and metadata on them and giving information on yourself (login information, details on your company, telephone number and potentially invoicing details). This amount of information contains personal data that we have to put a special emphasis on. We only manage personal data in order to fulfil our contractual commitments towards our users and customers for an amount of time that is reasonable for being able to provide you our services.
We try to sum everything up that you need to know on how we deal with information security and how we comply with the rules of the European Union General Data Protection Regulation (the GDPR).

WHERE DO WE STORE THE DATA?

iBinder uses Microsoft Azure as solution provider for our data processing needs as well as for data storage. The contract and solution are load-based and scalable. Microsoft Azure is certified for ISO 27001 (Information Security Management) and ISO 27018 (Code of Practice for Protecting Personal Data in the Cloud). To learn more on the topic, please visit https://azure.microsoft.com.

HOW DO WE KEEP OUR CUSTOMERS' AND USERS' SECRETS AND LOG THEIR DATA?

There is an internal policy for customer secrecy that the Support Agents of iBinder follow. They are the guardians of all secrets and they never communicate the passwords of our users and customers over the phone. Instead, it is sent via e-mail to the address registered on the user's account. The iBinder Support Agents will not add participants or change participants' access rights in a project without written approval from the project administrator. No information about ongoing projects and connected participants will be given out by the Support Agents without written approval from the project administrator.
All logins to iBinder are logged and can be traced if necessary. Document upload and removal are also logged and can be traced. There are five people at iBinder AB who can access the iBinder servers to perform system maintenance and secure availability and functionality in the iBinder system.

HOW DO WE COMMUNICATE WITH THE SERVERS?

All communication to and from iBinder.com's servers is done by encrypted https traffic, where 128 bit SSL is used for the encryption. Calls to the servers are logged and can be traced if needed.

WHAT IS GDPR?

The GDPR replaces earlier national data privacy legislations in the European Union member states. To a large extent, the rules of the GDPR are a continuation of the current legislation but the GDPR also contains some important changes to strengthen the protection of personal data of individuals.
The GDPR makes a difference between the roles of data controller and data processor.
iBinder is data controller for the processing of personal data necessary to provide the Service since iBinder decides purpose and means of the processing of this data. This means that iBinder is the data controller of, for example, contact details to individuals that have user accounts in iBinder.
The customer is data controller for processing of personal data in its business. This means that the customer paying license fees to iBinder or iBinders' partners is data controller for personal data in digital binders in the Service. iBinder is, in this situation, data processor to the customer.

WHICH KIND OF AGREEMENT IS THERE BETWEEN THE PROCESSOR AND THE CONTROLLER?

A data controller using a data processor must enter into a written data processor agreement with the data processor when they use iBinder. The data processor agreements regulate the relationships and the rights and obligations of the data controller and data processor as regards personal data. The requirements of the data processor agreement are set out in article 28 of the GDPR.
We adapted our data processor agreement to the GDPR – this is an agreement that sets the rules every time someone uses our service or signs up to it. – and made it a part of our General Terms and Conditions.

If you require further information on which section of our Data Processing Agreement corresponds to the requirements of the GDPR, please send us a written request to our support or general inquiry e-mail address that you find on our webpage and we will be happy to inform you!

WHY IS GDPR SO IMPORTANT?

The GDPRs starts to apply on 25th May 2018, replacing the current national legislative acts within the data protection area such as the Swedish Personal Data Act (PUL). The GDPR contains important news; however the majority of the current rules will continue to apply.

What is new in GDPR?

A number of new rules will be introduced with the GDPR.
Here are a couple of highlights that are relevant for iBinder:

- the potential sanction fee levels will be raised,
- personal data breaches shall be reported to the Swedish Data Protection Authority
- requirements of so-called privacy by design will be imposed personal data processed in e.g..email or word processor documents will become regulated to a larger extent than today (This has been an exception in PUL before, called unstructured processing of personal data)
- personal data incidents must be reported to the Data Inspection Board within 72 hours and the board can issue administrative fines of up to 4 per cent of the global turnover or at a maximum 20 million SEK for breaches of the law.
- data processors will have their own regulatory obligations, primarily regarding information security in relation to the personal data processed.

What are the most important data privacy principles in the GDPR?

All processing of personal data under the GDPR must comply with a set of data privacy principles.

Lawfulness, fairness and transparency

We are processing personal data with a legal basis and all our users (the data subjects) are entitled to clear and concise information about how their personal data is processed. To learn more on the legal grounds, please check the GDPR.

Purpose limitation

We collect and process personal data for specific, expressed and legitimate purposes and don't process it further in any other way.

Data minimisation

The personal data that we process is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

We keep the personal data accurate and up to date, where necessary.

Storage limitation

We keep personal data in a form which permits identification of our users for no longer than is necessary for the purposes for which the personal data are processed.

Integrity and confidentiality

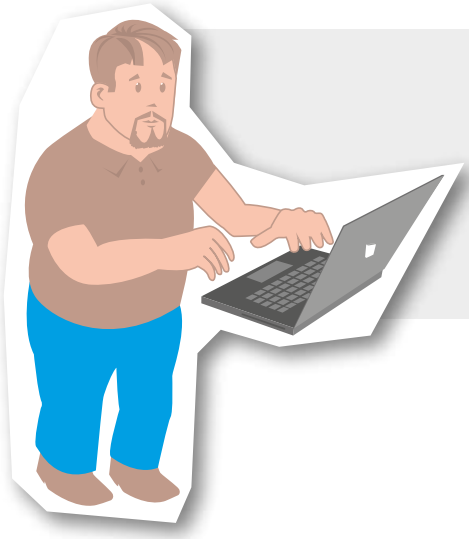
We process personal data in a manner that ensures appropriate security of it, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

We are responsible for, and can demonstrate compliance with the principles set out above. Our users as data controllers are accountable the same way.

What are the controller and the processor responsible of?

iBinder is data controller for some data processed but the paying customer is responsible for all personal data processed in the digital binders. The data controller can never transfer the regulatory responsibility as such, but can oblige another party to ensure fulfillment, for example in a data processor agreement.
The data controllers are collecting the users' consent (or make sure that there is a lawful basis of the collection oand processing of personal data). They are also responsible for the purpose limitations, the provision of necessary and accurate information and the accuracy of information on the data subject. They ensure privacy by design and are deleting personal data when it is necessary. The data processors process the personal data according to instructions and assist the data controllers to meet their obligations. It means that they make it easy for the controller to report on a breach for example. Both the data controller and the processor are responsible for the information security, the provision of limited access to personal data and the execution of the data processor agreement. The damages and administrative fines are also managed by both of them.



To learn more on data processors and controllers, please check the GDPR.

If you want to learn more about how we handle personal data, or just want to have a chat on binders, constructions and the life of architects and builders, feel free to contact our team! To find contact information, please go to www.iBinder.com.

iBinder
BUILDING ON SIMPLICITY