Privacy policy

Table of contents

Purpose of the privacy policy

The purpose of the privacy policy is to set out in a clear and comprehensible manner the data protection and data management principles of WIEDENMANN LTD (hereinafter referred to as the “Data Controller”) and the data protection and data management policy of the Data Collector, which the Data Controller acknowledges as binding on itself. In developing these rules, the Controller has taken particular account of the European Union Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council and the resolutions of the “working party 29”, as well as the relevant national provisions of the application and its laws, regulations and recommendations for harmonisation.

The purpose of this statement is also to ensure that in the performance of the specific tasks of the Data Controller, as set out by its founders, the rights of Data Subjects to their personal data and their access to it are guaranteed to all natural persons – regardless of their nationality or place of residence – in all areas of the services it provides. It should be transparent that the Controller ensures that Data Subjects who come into contact with them have fundamental freedoms, in particular the right to privacy when processing their personal data electronically, by machine and manually (data protection).

The Data Controller is committed to protecting the personal data of its customers and partners, keeps their personal data confidential and takes all data security, data protection, technical and organisational measures to prevent accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to the personal data processed.

Data Controller's data

Name: WIEDENMANN LTD.
Headquarters: 9343 Beled, Rákóczi út 228.
Company registration number: 08 09 002733
Tax number: 11121615208
Central email: beled@wiedenmann.de

Data protection officer of the Data Controller
Name: Eszter Boros
Email address: Eszter.boros@wiedenmann.de
Phone number: 00 36 30 862 4272

Website data management

Data related to online administration

For the website, the Controller may provide an interface where the Data Subject’s personal data may be recorded for the purpose of contacting the Data Subject.
Purpose of processing: contacting
Data processed in the data management: contact details
Legal basis for processing: consent of the Data Subject

Retention period of data processed in the data management: until consent is withdrawn
In such cases, the purpose of the processing and the acceptance of the processing will be clearly indicated on the website. The fact and the date of acceptance can be evidenced by the ticking of the acceptance checkbox with the active consent of the Data Subject and its logged date.

Third party analytics cookies

The Data Controller also uses Google Analytics as a third party cookie on its website. By using Google Analytics for statistical purposes, the Controller's server collects information about how visitors use the website. The data is used to improve the website and the user experience. These cookies will also remain on the visitor's computer or other browsing device, their browser, until they expire or until they are deleted by the visitor. The site will not remember any identifier or password even if cookies are enabled. Even if visitors accept cookies, they can still use the electronic services of the site in complete safety.

Physical storage locations of website data

In the case of a service involving the recording of personal data that may be authorised on the website, the Data Controller stores the data on the integrated IT system operated by the service provider that cooperates as data processor. The components of the system are located in the following geographical and physical locations:

Name of data processor	Address of data processor	Activity of data processor
1A Hosting Kft.	9700 Szombathely Király utca 21,	Webhosting service
LV Services Kft.	1211 Budapest, Weiss Manfréd út 5,	Webhosting service
ITD Informatika Zrt.	1211 Budapest, Weiss Manfréd út 5,	Webhosting service

IT storage and logical security of website data

The Data Controller processes personal data primarily in an adequately built and protected IT system. In the course of the operation of the IT system, it shall ensure an appropriate level of the basic information security attributes of the data stored, processed and transmitted on it, such as the following: integrity of the data, the originality and unchangingness of the data is guaranteed; confidentiality, only those entitled to access the data have access to it, to the extent that they are authorised; availability, the data is accessible and available to the authorised persons for the expected period of availability. The data processor shall design and operate the protection measures in proportion to the level of protection of each protection measure, the risks posed to the data to be protected. From a data protection point of view, the protection measures shall be primarily aimed at protecting against accidental or intentional deletion, unauthorised access, intentional and malicious disclosure, accidental disclosure, loss or destruction of data.

Transmission of data on the website, processing of data, access to data

The data may be accessed primarily by internal staff of the Data Controller, data processor, to the extent permitted by the rules of access, the access control system and other internal DPA rules. The Data Controller may use third party processors to perform certain operations and tasks related to the data. The Data Controller shall not disclose the data and shall not share it with a third party. Data will not be transferred to third countries.

Data controller's general data management processes for partners' data processing

Data processing concerning partners and external stakeholders

Data management process	Purpose	Legal basis	Categories of Data Subjects	Categories of personal data processed	Planned retention period
Recording of contact details of interested parties, customers	Contact for business marketing purposes	Legal basis for consent	Business enquiries	Identity and contact details	Until the Data Subject's request for erasure
Recording of financial identification data relating to the accounting and tax arrangement of customers	Enforceability of warranty/guarantee claims, compliance with accounting and tax obligations	Legal basis for legal provision	Customers	Identifying data, contact details	Legal period
Recording of recorded audio and visual material of meetings conducted by means of telecommunication	The purpose of recording meetings conducted with remote participation is to ensure the efficiency of business processes	Legal basis for legitimate interest	Employees, external experts, subcontractors, suppliers, customers	Image and audio recording	max 3 months
Recording of CCTV footage	Ensuring protection of property	Legal basis for legitimate interest	Employees, clients, contractors	Identity-related data	max 3 months

Record of business data of subcontractors, suppliers

Purpose of processing: Ensuring the Company's supplier business processes and related accounts, contracts registration.
Data processed in the data management:

- Identity-related data
- Contact details
- Identifying data
- Economic, financial data

Legal basis for processing: processing on the basis of legal provision
Retention period of the data processed in the data management: after the expiry of the obligation to provide analytical data as defined in the accounting legal environment, personal data will be deleted after the expiry of the supplier contracts and the exit from the network of contacts.

Record of contact details of interested parties, potential customers

Purpose of processing: Contacting and maintaining potential partnerships.
Data processed in the data management: contact details
Legal basis for processing: legitimate interest
Retention period of data processed in the data management: 10 years
In such cases, in accordance with the purpose of the processing, in all cases when the Data Subject objects, the controller will uphold the objection and delete the personal data.

Record of business and contact details of customers for whom the Company still has a warranty/guarantee obligation

Purpose of processing: In addition to the guarantee/warranty obligations, the purpose is to comply with the obligations imposed by the legal environment of accounting and taxation.
Data processed in the data management:

- Identity-related data
- Contact details
- Identifying data
- Economic, financial data

Legal basis for processing: compliance with legal obligations
Retention period of data processed in the data management: 10 years
In such cases, in accordance with the purpose of the processing, in all cases when the Data Subject objects, the controller will uphold the objection and delete the personal data.

Recording of audio and visual material of meetings conducted by means of telecommunications

Purpose of processing: Ensuring the full exploitation of the content of business meetings, discussions and technical content, while safeguarding the personal rights of the participants.
Data processed in the data management:

- Identity-related data

- Voice recording
- Image recording

Legal basis for processing: legitimate interest
Retention period of data processed in the data management: up to one year, until the purpose of the meeting is fulfilled

Recording of CCTV footage

The Company has installed and operates a security camera system on its territory. The camera system captures and records images of individuals within its scope, and therefore, under the relevant regulations, this activity is considered as data processing, while the Company is considered as the Data Controller in this respect. The camera recordings and the rules related to them are set out in a separate camera policy.
Purpose of processing: Effectively enhancing the security of the Company's assets.
Legal basis for processing: legitimate interest
Data processed in the data management:

- video recording

Retention period of data processed in the data management: 7 days

Rights of Data Subjects

Right to information and access

The Data Subject has the right to obtain from the Data Controller information and access to the processing of their personal data and, if such processing is ongoing, the right to access the personal data and the information listed in the regulation.
For example (but not fully listed):

- Purpose of processing
- Legal basis
- Retention period
- Categories of personal data processed
- Data processors used
- Recipients
- Transferring to a third country
- Enforceable rights
- Source of data processed

Right to rectification

The Data Subject has the right to obtain from the Data Controller, upon their request, the rectification of inaccurate personal data relating to them without undue delay.

Right to erasure

The Data Subject shall have the right to obtain from the Controller, upon their request, the erasure of personal data relating to them without undue delay, and the Controller shall be obliged to erase personal data relating to the Data Subject without undue delay if the

retention period of the data has expired or if the Data Subject's rights relating to the purpose of the processing permit or require so.

Right to be forgotten

If the Controller has disclosed the personal data and is obliged to erase it, it shall take reasonable steps – including technical measures –, taking into account the available technology and the cost of implementation, to inform the data processor that the Data Subject has requested the erasure of the links to or copies or replicas of the personal data in question.

Right to restriction of processing

The Data Subject shall have the right to obtain, at their request, the restriction of processing by the Controller if one of the following conditions is met:

- The Data Subject contests the accuracy of the personal data, in which case the restriction shall apply for a period of time which allows the Controller to verify the accuracy of the personal data;
- The processing is unlawful, and the Data Subject opposes the erasure of the data and requests the restriction of its use instead;
- the Controller no longer needs the personal data for the purposes of processing, but the Data Subject requires it for the establishment, exercise or defence of legal claims;
- the Data Subject has objected to the processing; in this case, the restriction shall apply for a period of time until it is established whether the legitimate grounds of the Controller prevail over the legitimate grounds of the Data Subject.

Right to data portability

The Data Subject has the right to receive personal data relating to them which they have provided to a Controller in a structured, commonly used, machine-readable format and the right to transmit such data to another Controller without hindrance from the Controller to which they have provided the personal data (...).

Right to object

The assertion of the legitimate interests of the Data Subject or of a third party is a specific legal remedy, but the Data Subject has the right to object at any time, on grounds relating to their particular situation, to the processing of their personal data.

Remedies of the Data Subject

If the Data Subject’s rights in connection with the processing of their personal data have been prejudiced despite their objection, they may exercise the following remedies:

- Request information about the processing of their personal data and request the rectification of their personal data
- They may request the erasure of personal data processed on the legal basis of consent. They may withdraw their consent.
- We will provide them with information on the data processed by us or by a processor on our behalf, the purpose, legal basis and duration of the processing.

- We will erase the User's personal data if the processing is unlawful, if the User requests it, if the purpose of the processing has ceased, if it is incomplete or inaccurate and cannot be lawfully rectified – provided that erasure is not prohibited by law–, or if the statutory period for storing the data has expired or has been ordered by court or the data protection commissioner.

The User may object to the processing of their personal data if

- the processing or transfer of the personal data is necessary solely for compliance with a legal obligation to which the Controller is subject or for the purposes of the legitimate interests pursued by the Controller, the recipient or a third party, unless the processing is required by law
- the personal data is used or transmitted for direct marketing, public opinion polling or scientific research purposes
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller.

The Controller shall examine the objection within the shortest possible time from the date of the request, but not later than one month, decide whether it is justified and inform the applicant in writing of its decision. If the Controller finds that the objection of the Data Subject is well-founded, it shall inform all those to whom it has previously disclosed the personal data. If the User does not agree with the decision of the Controller, they may challenge it in court within 30 days of its notification. The court shall deal with the case as a matter of urgency. The competent court shall be the court in the place where the Data Controller is established, but the action may also be brought – at the choice of the Data Subject – before the court in the place where the Data Subject resides.

Data Protection Authority

Complaints against possible infringements by the Controller may be lodged with the National Authority for Data Protection and Freedom of Information:
National Authority for Data Protection and Freedom of Information
Address: 1374 Budapest, Pf. 603.
E-mail: ugyfelszolgalat@naih.hu

Right to legal proceedings

Irrespective of the right to lodge a complaint, the Data Subject may also take legal action against the unlawful processing of their personal data or the infringement of their rights relating to their right to informational self-determination. In Hungary, legal proceedings may be brought before the competent court of the place of residence or stay of the Data Subject or before the competent court of the place where the Controller is established. You can find the responsible court according to your place of residence or stay at https://birosag.hu/birosag-kereso.

Interpretative definitions

In accordance with the definitions of Regulation (EU) 2016/679 of the European Parliament and of the Council:

“personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

“data processing” means any operation or set of operations which is performed upon personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“restriction of processing” means the marking of stored personal data for the purpose of restricting their future processing;

“profiling” means any form of automated processing of personal data by which personal data is used to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict characteristics associated with performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements of that natural person;

“pseudonymisation” means the processing of personal data in such a way that it is no longer possible to identify the natural person to whom the personal data relate without further information, provided that such further information is kept separately and technical and organisational measures are taken to ensure that no natural person who is identified or identifiable can be linked to that personal data;

“register system” means a set of personal data, structured in any way – whether centralised, decentralised, functional or geographical – which is accessible on the basis of specific criteria;

“data controller” means a natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of the processing are determined by Union or Member State law, the controller or the specific criteria for the designation of the controller may also be determined by Union or Member State law;

“data processor” means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of a controller;

“recipient” means a natural or legal person, public authority, agency or any other body to whom or with which personal data is disclosed, whether or not a third party. Public authorities that may have access to personal data in the context of an individual investigation in accordance with Union or Member State law are not recipients; the processing of those data by those public authorities must comply with the applicable data protection rules in accordance with the purposes of the processing;

“third party” means a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor or the persons who, under the direct authority of the controller or processor, are authorised to process personal data;

“data subject's consent” means a freely given, specific, informed and unambiguous indication of the data subject's wishes by which they signify, by a statement or by an act unambiguously expressing their consent, that they agree with the processing of personal data relating to them;

“privacy incident” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed;

“category of data subjects”

- Employees
- Users
- Subscribers
- Students
- Military personnel
- Customers (current and potential)
- Patients
- Minors
- Vulnerable persons
- Persons subject to or affected by official proceedings or measures
- Not yet known
- Other

“nature of the privacy incident”

- Phishing
- Electronic waste (personal data remains on outdated device)
- Loss or theft of a device
- Hacking of an IT system
- Loss or unauthorised opening of mail
- Loss, theft of a paper document or leaving it in a place that is not considered secure
- Improper destruction of a paper document
- Malicious computer programmes e.g. ransomware
- Unauthorised access to personal data
- Unauthorised oral communication of personal data
- Unlawful disclosure of personal data to a large public
- Sending personal data to the wrong recipient
- Other

“causes of the privacy incident”

- External, malicious act
- An external act that does not constitute bad faith
- Internal malicious act

- Internal act that does not constitute bad faith
- Other

“categories of personal data affected by privacy incident”

Categories of personal data
- Identity-related data
- Identity number
- Contact details
- Identifying data
- Economic, financial data
- Video recording
- Audio recording
- Official documents
- Location data
- Biometric data
- Data relating to criminal history, offences or penalties, measures

Categories of special data
- Data on racial or ethnic origin
- Data on political opinions
- Data on religious or other philosophical beliefs
- Data on membership of an interest representation organisation
- Data on sexual life
- Health data
- Genetic data
- Not yet known
- Other

“breach of confidentiality”
- Wider access than necessary or consented to by the data subject
- The data has become combinable with other data of the data subject
- The data may be processed in an unfair way for other purposes
- Other

“integrity breach”
- The data became modifiable despite the fact that it was archived outdated data
- The data is likely to have been modified into otherwise accurate data and used for different purposes
- Other

“availability breach”
- Loss of ability to provide critical services to data subjects
- Change in ability to provide critical services to data subjects
- Other

“likely impact of the incident on data subjects”

- Unauthorised unblocking of pseudonymisation
- Restriction of the rights of the data subject
- Discrimination
- Damage to reputation
- Financial loss
- Damage to the confidentiality of personal data protected by professional secrecy
- Identity theft
- Misuse of identity
- Loss of control over personal data
- Other

"genetic data" means any personal data relating to the inherited or acquired genetic characteristics of a natural person which contains specific information about the physiology or state of health of that person and which results primarily from the analysis of a biological sample taken from that natural person;
"biometric data" means any personal data relating to the physical, physiological or behavioural characteristics of a natural person obtained by means of specific technical procedures which allow or confirm the unique identification of a natural person, such as facial image or dactyloscopic data;

"health data" means personal data relating to the physical or mental health of a natural person, including data relating to the provision of health services to a natural person which contain information about the health of the natural person;

"representative" means a natural or legal person established or residing in the European Union, designated in writing by the controller or processor pursuant to Article 27, who represents the controller or processor in relation to the obligations incumbent on the controller or processor under this Regulation;

"undertaking" means any natural or legal person, regardless of its legal form, engaged in an economic activity, including partnerships or associations carrying on a regular economic activity;

"group of undertakings" means the controlling undertaking and the undertakings controlled by it;

"binding corporate rules" means the rules on the protection of personal data followed by a controller or processor established in the territory of a Member State of the Union in one or more third countries in relation to the transfer or series of transfers of personal data by a controller or processor within the same group of undertakings or the same group of undertakings engaged in joint economic activities;

"supervisory authority" means an independent public authority established by a Member State in accordance with Article 51;

"supervisory authority concerned" means a supervisory authority which is concerned by the processing of personal data for one of the following reasons:

- The controller or processor is established in the territory of the Member State of that supervisory authority;
- The processing significantly affects or is likely to significantly affect data subjects residing in the Member State of the supervisory authority; or
- A complaint has been lodged with that supervisory authority;