

Balanco Oy Corporate Customer, Supplier and Cooperation Partner Register Privacy Notice

Balanco Oy processes in its operations personal data concerning customer, supplier or cooperation partner companies and organisations in accordance with this privacy notice. This privacy notice sets out the information to be provided to the data subject as required by Articles 12–14 of the EU General Data Protection Regulation.

Balanco Oy may amend this privacy notice by publishing a new version of it on its website, for example, when legislation, authorities' instructions, case law or its own practices change. Data subjects will be separately informed by email of material changes in the processing of personal data. Other changes will not be separately notified unless required by legislation. This notice contains up-to-date information on our practices relating to the processing of personal data.

1 Controller's contact details in data protection matters

Controller	Balanco Oy, Business ID: 2699983-6 ("Balanco", "Company" or "Controller")
Contact in all data protection matters	The Data Subject may contact the Controller in all matters concerning data protection as follows: Balanco Oy Address: Robert Huberin tie 16 C, 15100 Vantaa Niia Ylilammi tel. 050 576 0333, tietosuoja@balanco.fi

2 Data Subjects

The Controller collects and processes personal data concerning the decision-makers, contact persons and representatives ("Data Subjects") of the Controller's current and potential customers, supplier or cooperation partner companies and organisations ("Company")

3 Personal data collected

The Controller collects and processes the following personal data concerning Data Subjects:

Data group	Description	Where the data is collected and updated from
Basic information	Company information (including invoicing and delivery information), name, title or profession, position or role in the Company, work-related contact details (postal and visiting address, email address, telephone number), year of birth, gender, native language,	- Data Subject - Company - Public and private registers, such as the Trade Register, Posti, Fonecta, and Asiakkuusmarkkinointiliitto

	service language, preferred method of contact	
Customer due diligence and verification data (information concerning the persons referred to in the Act on Preventing Money Laundering and Terrorist Financing 28.6.2017/444)	Data for verifying, identifying and individualising the identity of the Data Subject, personal identity code, date and place of birth, nationalities, place of residence, municipality of residence, copy of passport or other personal identification document	• Data Subject • Banks' identification services, other providers of electronic signature and identification services, when the Data Subject identifies themselves in an electronic contract/order process or registers for an electronic transaction service
	Information related to the prevention of money laundering, prevention of terrorist financing and PEP information concerning political influence	• Data Subject • Consolidated sanctions lists of the EU Commission and the UN Security Council • Companies providing sanctions and PEP information • Public and private registers, such as Digi- ja väestövirasto, the Trade Register, Posti
	Information on the customer's activities, nature and scope of business, financial position, grounds for the transaction or use of the service and information on the origin of funds	• Data Subject • Controller • Other credible and reliable information sources
	Information on suspicious transactions	
Information concerning suspected offences	Information on suspicions concerning other offences or misconduct	• Data Subject • Controller and its information systems
Credit information	Credit information concerning the person responsible for the Company	• Credit information companies in connection with a creditworthiness check
Marketing information	• Information concerning the Data Subject's duties and position in business life or in a public role, professional interests	• Data Subject (e.g. in connection with service events or participation in events) • Controller

	• Information on requests for quotations and enquiries made by the Data Subject and on quotations and other pre-contractual marketing measures and contacts sent to the Data Subject • Consents, prohibitions, restrictions and authorisations given by the Data Subject concerning the use of data and direct marketing • Other information provided by the Data Subject	• Company's website • Public and private registers, such as the Trade Register, for example, and contact information services, such as Suomen Asiakastieto Oy, Fonecta Oy, Posti Oy
Usage data of electronic services	Usage history and log data recorded in connection with the use of electronic services	• Data Subject • Controller's information systems
	Newsletter usage data email address, information concerning sending, receipt and reading	• Data Subject • Information systems of the Controller and its subcontractor
	Usage and browsing data of online services: page from which the user has entered the Controller's website, device model, unique device and/or cookie identifier, data collection channel (Internet browser, mobile browser, application), browser version, IP address, session identifier, session time and duration, screen resolution and operating system, country-/city-level location	• Data Subject (through cookies, advertising identifiers, etc. information on the use of Internet and mobile services and newsletters).
Information concerning the customer or other relationship	Communications and other actions in the relationship between the Controller and the Company, newsletter subscription and cancellation information	• Controller • Data Subject
Event organisation information	Participation information, e.g. invitation, registration and participation information relating to events, competitions, prize draws and	• Data Subject

	other events organised by the Controller	
	Health information: necessary dietary and accessibility information	• Data Subject
	Photographs, videos taken at events	• Controller
Profile and classification information	Classified segments and profiles created on the basis of analysis and profiling of the information described above for the purposes of processing in accordance with this notice.	The information is generated automatically on the basis of the information in the customer register

Information concerning the Company is not personal data

Legal acts and documents between the Controller and the Company (e.g. electronic transaction forms, requests for quotations, quotations, orders, agreements, etc.) carried out by the Data Subject on behalf of the Company as its representative, as well as the Data Subject's information contained therein, are not personal data but information describing the Company, and the Data Subject's rights and data protection legislation do not apply to them.

4 Legal bases and purposes of processing personal data

The personal data of Data Subjects referred to in section 3 is processed on the legal bases and for the purposes presented in the following table:

Purpose of processing	Data groups processed	Legal basis
Advertising and targeting of the Controller's services and events related to the Data Subject's work duties in the Controller's own and other Internet and mobile services and applications; direct marketing and its targeting by telephone, letter, email, text message and otherwise electronically; conducting opinion and market research, organising marketing competitions and other events	• Basic information • Marketing information • Information concerning the customer or other relationship • Usage data of electronic services • Profile and classification information • Event participation information	• Controller's legitimate interest in conducting business and marketing its services (Data Protection Regulation, Article 6(1)(f)) • With regard to the use of online service usage and browsing data, the Data Subject's consent to the use of cookies (Act on Electronic Communications Services, section 205)
• provision of customer, support and other services • handling contacts, managing, developing and maintaining the customer relationship	• Basic information • Marketing information	Controller's legitimate interest based on the right to conduct business and on the customer, supplier or other relationship between the Controller and the Company

- customer communications and contacts by letter, telephone, email, text message or other electronic means - customer satisfaction and other customer research and surveys - development of business and services	- Information concerning the customer or other relationship - Usage data of electronic services - Event participation information - Profile and classification information	(Data Protection Regulation, Article 6(1)(f))
Fulfilment and documentation of customer due diligence obligations, including preparation and maintenance of a customer risk assessment, prevention of money laundering and terrorist financing, and fulfilment of the reporting obligation and duty to obtain information referred to in law	- Basic information - Due diligence and verification data	Compliance with a legal obligation (Data Protection Regulation, Article 6(1)(c), Act on Preventing Money Laundering and Terrorist Financing; Act on the Fulfilment of Certain Obligations of Finland as a Member of the United Nations and of the European Union and provisions issued pursuant thereto)
Provision of the newsletter service	Newsletter subscription, usage and cancellation information	Performance of the Data Subject's newsletter subscription (Data Protection Regulation, Article 1, point 6 b))
Organisation of events	- Basic information - Event organisation information	Controller's legitimate interest based on the right to conduct business (Data Protection Regulation, Article 6 (1)(f))
	Health information	Data Subject's consent (Data Protection Regulation, Article 6(1)(a))
Controller's communication concerning events in the media, on the Internet, in social media	Photographs, videos taken at events	Data Subject's consent (Data Protection Regulation, Article 6(1)(a))
Ensuring information security	- Basic information - Usage data of the Controller's electronic services	Compliance with a legal obligation (Data Protection Regulation, Article 6(1)(c) and Article 32, Act on Electronic Communications Services)

Detection, prevention and investigation of fraud and other offences and misconduct	The data mentioned in section 3 necessary for the purpose in each case and information concerning suspected offences	Controller's legitimate interest in ensuring the prevention of offences directed at it and other parties (Data Protection Regulation, Article 6(1)(f))
Performance of statutory duties concerning the Company and Data Subjects and other statutory duties of the Controller	All data mentioned above in section 3 that is necessary for each statutory duty in each case	Compliance with a legal obligation, e.g. reporting to authorities (Data Protection Regulation, Article 6(1)(c))
Analysis, statistics and profiling for the development of services and the customer relationship and for marketing	All data mentioned above in section 3 that has been stated to be processed for each purpose in accordance with this notice	Controller's legitimate interest based on the customer relationship (Data Protection Regulation, Article 6(1)(f))
	Usage and browsing data of online services	Data Subject's consent to the use of cookies (Act on Electronic Communications Services, section 205)

The Controller does not use automated decision-making in its activities concerning Data Subjects.

5 Disclosure of Data

The Controller may disclose information in the register to companies belonging to the same group as the Controller and to cooperation partners when necessary for fulfilling the purposes of the register, e.g. provision and invoicing of services, management of the customer relationship and marketing.

Personal data is not disclosed to other parties without the consent of the Data Subject except where it is necessary for the Controller to fulfil its statutory obligations, in connection with legal proceedings, at the request of authorities or as part of business arrangements.

6 Transfer of data for processing by subcontractors

The Controller has the right to use subcontractors in the processing of personal data in accordance with this notice. In such cases, personal data may be transferred to subcontractors to the extent necessary for the provision of the subcontractor's services. Each subcontractor processes personal data only to the extent necessary for carrying out the subcontractor's duties. Subcontractors process personal data on behalf of and for the account of the Controller in accordance with the Controller's instructions. Subcontractors are bound by agreements concluded with the Controller concerning the processing of personal data, including terms concerning confidentiality and information security.

The Controller uses subcontractors, among other things, for the following tasks:

Subcontractor or group	Task
Advertising and marketing agencies	marketing, analytics
Financial administration service providers	accounting and other financial administration services
ICT suppliers	Information system services, cookie management, telecommunications services, other electronic

	communication services and information security services
Google Inc.	Statistical monitoring of Internet services is carried out by Google Inc. on behalf of the Controller in accordance with the cookie consent given by the Data Subject. Google may also use information collected through cookies for its own marketing purposes in accordance with the cookie consent and its own terms of use and privacy terms. Google itself is responsible for its own cookies and for information collected through them for its own use; see further information at: Google's cookie policy

7 Transfer of data to third countries

As a general rule, we process personal data within the European Union (EU) and the European Economic Area (EEA). However, the Controller may disclose or transfer personal data to a country outside the EU/EEA when a service provider or partner processing personal data operates wholly or partly in a third country. Unless the European Commission has decided that the level of data protection in the destination country is acceptable, the Controller ensures appropriate data protection by concluding written agreements with the recipient using the standard contractual clauses approved by the European Commission or another lawful procedure. In such cases, the Controller ensures the necessary safeguards and implements, to the extent necessary, additional measures to protect personal data as required by applicable legislation. The standard contractual clauses can be found in the [European Commission Standard Contractual Clauses \(SCC\)](#)

8 Processing of personal data concerning users of the Controller's social media

The Controller's internet website uses social media functions (i.e. social plugins), such as Facebook, Instagram and LinkedIn buttons, which direct users to social media pages maintained by the Controller. Social media services share user information with the Controller in accordance with their privacy notices and the consents given by users, e.g. comments and links concerning the Controller's websites shared by the user in the media, as well as information contained in the user's public profile. The Controller processes personal data received through its social media pages on the basis of legitimate interest only for the Controller's own purposes, such as informing about new products, services or offers, carrying out competitions and prize draws, receiving feedback, purchasing advertising from the social media service, measuring the reach of pages or advertisements, or providing customer service on social media pages. The Controller does not process the information outside social media, and information shared by them is not combined with the Controller's other information or registers without the user's consent.

Social plugins are the responsibility of the company providing them. They are primarily responsible for compliance with data protection legislation and for ensuring information security and the implementation of the Data Subject's rights in the service. The privacy practices of social media services can be reviewed and their privacy settings managed on a service-specific basis:

- [Facebook and Instagram](#)
- [LinkedIn](#)

9 Principles of register protection

Only persons who need the information for carrying out their work duties are entitled to use the data. Personnel processing personal data have been provided with training and instructions concerning data protection. Personnel and subcontractors processing the data are bound by confidentiality obligations. Information concerning suspected offences is stored separately from other information concerning Data Subjects.

Personal data is stored in locked premises corresponding to the level of protection required for the data, which are monitored by automatic access control. The protection of electronically stored data is based on access rights management, user identification, technical protection of databases and servers, e.g. firewalls and other information security software, data encryption, protection of data communications, data backup, as well as collection of log data and monitoring of information security events.

10 Personal data retention periods

Data group	Retention period
Due diligence and verification data	5 years from the end of the customer relationship
Data collected on the basis of consent	For as long as the consent given by the Data Subject remains valid
Recordings of calls and remote meetings	12 months from recording
Usage data of electronic services collected through cookies	In accordance with the periods stated in connection with cookie consents
Other Usage data of electronic services	No more than 5 years after the end of the customer, supplier or other relationship between the Controller and the Company or after the Controller has received information that the Data Subject is no longer employed by the Company
Basic information and Marketing information	Permanently within the limits permitted by law, unless the Data Subject has prohibited the processing of the data
Anonymised data	Data from which a person cannot be identified may be retained permanently
Backups	In accordance with the Controller's normal retention and deletion schedules
Other personal data	No more than 2 years after the end of the customer, supplier or other relationship between the Controller and the Company or after the Controller has received information that the Data Subject is no longer employed by the Company

Data may be retained after the above-mentioned retention periods for the establishment, exercise or defence of legal claims until the claims have been finally resolved. If personal data is processed for the fulfilment of statutory obligations, it is retained in accordance with legal requirements. The obligation to retain personal data is provided for, for example, in legislation concerning accounting and money laundering.

The Controller regularly assesses the necessity of retaining personal data, e.g. identification and verification data and documents no later than three years after the previous review of the necessity of retention. In addition, the Controller takes reasonable measures to ensure that personal data concerning

Data Subjects that is incompatible with the purposes of processing, outdated or inaccurate is not retained in the register.

11 Rights of the Data Subject

The Data Subject has the right to access the information concerning themselves stored in the personal data register and to request the rectification or deletion of inaccurate, outdated, unnecessary or unlawful information.

The Data Subject does not have the right of access to Information concerning suspected offences. At the request of the Data Subject, the Data Protection Ombudsman may review the lawfulness of the processing of such information.

The Data Subject has the right at any time to cancel the newsletter subscription and the right to withdraw consents previously given for the processing of their personal data. Withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal of consent.

The Data Subject has the right to prohibit the use of their data for direct marketing, opinion and market research, including related profiling.

Where the processing of personal data is based on legitimate interest, the Data Subject has the right to object to the processing of their data on grounds relating to their particular personal situation. In connection with the request, the Data Subject must specify the particular situation on which the objection is based.

The Data Subject may request restriction of the processing of their personal data, for example complete or partial suspension where, in the Data Subject's opinion, there is uncertainty regarding the accuracy of the data or its processing, until the uncertainties concerning the data have been clarified and resolved.

If the Data Subject has provided their personal data to the Controller and the processing is based on consent or a contract, they have the right to receive this data in a structured, commonly used and machine-readable format and the right to transfer the data to another Controller in accordance with applicable legislation.

The Data Subject may exercise the above-mentioned rights by sending requests concerning them in writing or by email to the Controller (contact details are provided at the beginning of the notice). The Controller may, if necessary, ask the Data Subject to specify their request in writing and prove their identity.

The Data Subject has the right to lodge a complaint concerning the processing of personal data with the Data Protection Ombudsman.