

Privacy Policy of PCB Baltic UAB

PCB Baltic UAB (hereinafter – *Data Controller*) respects your privacy and undertakes to ensure it in accordance with the following Privacy Policy (hereinafter – *Policy*). Data Controller hereby seeks to provide you with detailed information about the processing of your personal data, regardless of whether you cooperate with the Data Controller in person, by electronic means (for example, using the Data Controller's website or by email), or by any other means of your choice.

Data Controller undertakes to ensure transparency and provide clear information about personal data types being processed, purposes of the processing, storage period of personal data, and legal basis of such processing and other information that has to be presented by the Data Controller pursuant to the applicable legislation.

Read this Policy carefully and, should you have any questions, contact the Data Controller by one of the following means listed at the end of the Policy.

PCB Baltic UAB is a manager of *www.pcbbaltic.lt* website.

Details of the Data Controller:

PCB Baltic UAB

Registration No. 300861592

Address: Nadruvos 10, LT-06228 Vilnius

E-mail: sales@pcbbaltic.lt

We hereby confirm that your data will be collected in accordance with the applicable requirements of the European Union and the Republic of Lithuania legislation, instructions of the controlling institutions, and we will employ all reasonable technical and administrative measures to protect the data of website visitors collected by the Data Controller from loss, unauthorised use and/or alteration. Employees of the Data Controller undertook in writing not to disclose or distribute the information obtained at the workplace, including information about visitors of the website/social network, to third parties.

Persons who are under 14 may not provide any personal data on our website. If you are under 14, you are required to obtain consent of your parents or other legal guardians prior to providing personal data.

Terms used in the rules are understood as defined in the General Data Protection Regulation No. 2016/679 (EU).

It is very important that you carefully read the Policy, since you agree to the terms provided herein every time you visit the website. If you do not agree to these terms, please stop visiting our website, using its contents and/or our services.

Your personal data, i.e. any information about you that enables the Data Controller to recognise you, are obtained by various means:

- You can provide the information (personal data) yourself (for example, by filling out the inquiry form, calling the Data Controller, subscribing to our newsletters, or contacting the Data Controller by other means);
- The information about you can be collected automatically (as you visit our website (by means of cookies and similar technology), the Data Controller's social network accounts on Facebook, LinkedIn, Google+, Youtube), Data Controller's office, representative offices and/or exhibition booths);

You can provide your personal data directly to the Data Controller. This is normally the case, where you:

- provide your data to obtain information about the Data Controller's goods/services;
- make requests or claims;
- subscribe to the Data Controller's newsletters or other communication;
- participate in surveys.

Information about you can be collected automatically. This is normally the case, where you:

- submit inquiries via the Data Controller's social network accounts;
- use the website (data are collected by means of cookies and similar technology. For more information about the cookies used by the Data Controller, please see below);
- make public posts on social network platforms monitored by the Data Controller;

to the extent this is permitted by the applicable legislation, the Data Controller may obtain information about you from third parties.

Data Controller may aggregate the information obtained from you, public and commercial sources with other information obtained from you or about you.

Even though the Data Controller makes every effort to minimise the information collected about you, for the purpose of his activities, the Data Controller collects the following information:

- information that is necessary to provide services/supply goods of the Data Controller to you;
- information provided by you in your inquiries;
- information provided by you when calling the Data Controller;
- information necessary to identify you and make sure that you are authorised to enter into agreements;
- information about your behaviour on the website;
- structured information about the behavioural habits of the visitors on the website;

Detailed information about ways of processing and types of data being processed is presented in the next section.

You can choose to refuse to provide certain information (for example, information requested in the inquiry form) to the Data Controller, but in such event, the Data Controller will be fully or partly unable to provide his services to you.

The information referred to above is processed for the following purposes:

- entry into and performance of purchase and sale agreements and other agreements;
- providing information related to your orders, service requests, requests for goods, etc.;
- marketing purposes*, for example, presenting personalised advertisements and sponsor content and sending information about promotions, assessing and analysing the market, clients, products and services (including surveys of your opinion about the products and services, surveys of clients/partners, contests or promotions, to the extent this is permitted under the laws);
- obtaining information about the use of our products and services so that we can improve them and develop new content, products and services;
- defending our interests in courts or other institutions.

Please be informed that the Data Controller may send advertising information by email about other similar products or services to his clients/potential clients or persons who filled out the order form, and you may refuse to receive our direct marketing materials now or later at any time; to this end, contact us by email sales@pcbaltic.lt or click the refusal link in the newsletter.

Your personal data are processed in accordance with one or several legal bases:

- compliance with statutory requirements;
- performance of an agreement signed with you;
- legitimate interests of the Data Controller, unless your private interests override them;
- in certain cases, your consent.

Legal basis for our processing of your personal data for the appropriate purposes as well as types of personal data being processed are presented below:

- Name, surname, national identification number, phone, address, email address. Collected for the purposes of signing and performing purchase and sale and other agreements. Legal basis – performance of agreements signed with you; compliance with the statutory requirements.
- Name, surname, phone, email, payment information, other information that may be necessary during the provision of services. Marketing purposes*, for example, presenting personalised advertisements and sponsor content and sending information about promotions, assessing and analysing the market, clients, products and services (including surveys of your opinion about the products and services, surveys of clients/partners, contests or promotions, to the extent this is permitted under the laws). Legitimate interest – providing information about any identified defects/malfunctions and other services, events, news and other relevant information; greeting you.
- IP address, operating system version and parameters of your device used to access the content, your session time and duration, and any information stored by means of cookies set up by us in your device, or information about the nearest WiFi access points and mobile network towers, which can be forwarded to us as you use the contents of our website. Collected to obtain information about the use of our products and services so that we can improve them and develop new content, products and

services. We process your personal data for this purpose with the legitimate interest of monitoring the quality of our services, developing and improving the content of our website, and ensuring security of our website.

- General information about candidates: name, surname, date of birth, place of residence or address thereof, email address and/or phone number, information about the candidate's work experience (workplace, employment period, position, responsibilities and/or achievements), information about the candidate's education (educational institution, period of study, education and/or qualifications acquired), information about ongoing training (completed training, certificates received), language, information technology, driving skills, other competencies, other information provided by you in your CV, letter of motivation or other application documents. Recommendations, employers' feedback: person recommending or reviewing the candidate, their contact details, recommendations or feedback. Candidate assessment information: summary information about interview with the candidate, comments and opinions of the person(s) selecting the candidates, test results of the candidates. Collected for the purposes of assessing and employing candidates applying for vacant positions. Legal basis – your consent.
- Purpose – defending our interests in courts or other institutions. Depending on the action or claim made, all the personal data available to us and listed in this Policy may be processed for this purpose. Legal basis – compliance with the statutory requirements; legal interest – defence in case of any actions and claims.

In cases, where the Data Controller cannot rely on one of the above legal bases, he will ask for your consent prior to processing your personal data (depending on the circumstances and context).

In cases, where the Data Controller processes your personal data for purposes other than those specified herein, the Data Controller will inform you by a separate notice.

If you provide the Data Controller with personal data of other persons associated with you, you should inform them and, if necessary, obtain consent of these persons and introduce them to this Policy. Data Controller may also collect your personal data, if you are a representative of the Data Controller's client that is a legal entity.

Data Controller may transfer your personal data:

- to representative offices of the Data Controller;
- credit and other financial institutions operating in Lithuania;
- state, municipal and legal enforcement institutions;
- companies that provide services on the Data Controller's request;
- other duly selected business partners of the Data Controller;
- other parties, where this is required under the laws or necessary to secure legitimate interests of the Data Controller.

Currently, companies that provide services on the Data Controller's request are as follows: IT service providers, couriers, advertising agencies, auditors, lawyers. Opportunities of such companies to use your information are limited: they cannot use this information for purposes other than the provision of services to the Data Controller.

To receive direct marketing offers from the Data Controller and/or Data Controller's business partners, you will be asked to give your consent.

Other parties that may receive information about you available to the Data Controller, where this is necessary for the purpose of securing our legitimate interests, are public authorities, law enforcement officers, courts, etc.

Sometimes Data Controller may have to transfer your personal data to other countries, which may apply lower levels of data protection. In such event, we will do all in our power to ensure the security of personal data being transferred.

On very rare occasions (for example, where you have special requests regarding our products), the Data Controller may be forced to transfer your personal data to countries outside the European Economic Area.

In the event of transferring your personal data to countries outside the European Economic Area, the Data Manager will inform you hereof and make sure that one of the following safety measures are applied:

- Agreement signed with the data recipient will be based on the standard contractual clauses approved by the European Commission.
- The data recipient will be established in a country recognised by the European Commission as applying adequate data protection standards.
- Approval from the Data Protection Inspectorate.

Data Controller has introduced reasonable and appropriate physical and technical measures to protect the information collected for the purposes of content/service provision. However, keep in mind that, even though we take the appropriate measures to secure your information, there are no fully secure websites, online operations, computer systems or wireless connections.

Data Manager will store your personal data to the extent necessary to achieve the specified purpose. Once the specified purpose is achieved, your personal data will be deleted, except in cases where the applicable legislation requires the Data Controller to store information for tax purposes or the data may be required for pre-trial investigation, but, in any case, the storage period will not exceed 10 years. Once this period expires, data will be deleted in a way that they cannot be reproduced.

Personal data are normally stored for the following periods:

- Data in payment, purchase and sale, and other agreements – 10 years after the payment operation.
- Data provided by candidates to vacant positions – 6 months after the end of the selection procedures.
- Personal data used for marketing purposes – as long as you are an active client of the Data Controller and 2 years after your last visit at the Data Controller or last actions in the Data Controller's website.
- IT system logs – at least one year.
- Analytical data – usually, these data are collected automatically as you use the website, and anonymised/aggregated immediately after receipt thereof.

Data subjects whose data are processed in the course of the Data Controller's activities have the following rights (depending on the situation):

- The right to be informed about the processing of their data (right to know).
- The right to have access to their data and ways of processing thereof (right of access).
- The right to rectification or, depending on the purposes of the processing, alteration of incomplete personal data (right to rectification).
- The right to erasure of data or suspension of the processing activities (except storage) (right of erasure and right to be forgotten).
- The right to request that the Data Controller limits the processing of personal data due to one of legitimate reasons (right to limitation).
- The right to transfer the data (right to data portability).
- The right to object to the processing at any time, where such processing is carried out in the public interest or this is necessary to secure legitimate interests of the Data Controller or third parties. For the Data Controller to process personal data, he is required to prove that the data are being processed for compelling legitimate reasons that override interests of the data subject (right to object).
- Lodge a complaint to the State Data Protection Inspectorate.

Data Controller may refuse to allow you to exercise the above rights, where in cases provided for in the laws, it is necessary to prevent, investigate and identify crime and breaches of integrity or professional ethics, as well as protect rights and freedoms of the data subject or other persons.

Your rights will be enforced upon prior identification in person or by email.

You have the following rights:

- The right to be informed about the processing of their data (right to know). The right to receive information about the processing of your data in a concise, simple and clear manner prior to the processing of your personal data.
- The right to have access to their data and ways of processing thereof (right of access). Following your identification, the Data Controller will provide you with information, provided that this does not interfere with rights and freedoms of other persons. This means:
 - confirmation that the Data Controller processes your personal data;
 - presentation of the list of your personal data being processed;

- presentation of purposes and legal basis of the processing of your data;
- confirmation whether the Data Controller transfers the data to third countries and, if so, disclosure of the protection measures taken;
- disclosure of the source of your personal data;
- information as to the application of profiling;
- disclosure of the data storage period.
- The right to rectification or, depending on the purposes of the processing, alteration of incomplete personal data (right to rectification). Applies if the information available to us is incomplete or inaccurate.
- The right to erasure of the data (right to be forgotten). Applies if:
 - The information available to the Data Controller is no longer needed for the specified purposes;
 - Data are processed based on your consent and you withdraw the consent;
 - Data are processed on other legitimate grounds and, on your request, it is found that your private interests prevail;
 - Information has been obtained by unlawful means.
- The right to suspend the processing of personal data (except storage). This right may be exercised for the period during which we analyse the situation, i.e.
 - if you contest the accuracy of the information;
 - if you object to the processing of personal data, where this is carried out on the basis of legitimate interests;
 - Data Controller uses the information in an unlawful manner, but you object to its erasure;
 - Data Controller no longer needs the information, but you request that it is stored due to legal dispute.
- The right to request that the Data Controller limits the processing of personal data due to one of legitimate reasons (right to limitation). You may object to the Data Controller's use of your personal data for the purpose of direct marketing.
- The right to data portability. This right may be exercised if you provided your data and the Data Controller processes them by automatic means based on your consent or agreement concluded with you.
- The right to object. This right may be exercised, where such processing is carried out in the public interest or this is necessary to secure legitimate interests of the Data Controller or third parties. For the Data Controller to process personal data, he is required to prove that the data are being processed for compelling legitimate reasons that override interests of the data subject.
- Lodge a complaint to the State Data Protection Inspectorate (www.ada.lt).

Request for the exercise of the above rights and complaints, notices or other requests can be submitted to the Data Controller by email: sales@pcbbaltic.lt, regular mail: Nadruvos 10, LT-06228 Vilnius, or to the Data Controller in person.

Data Controller will reply to your request not later than within 30 (thirty) calendar days from the date of receipt thereof. In exceptional cases (where additional time is required), the Data Controller may extend the period of presenting the requested data or examining other requests to 60 (sixty) calendar days from the date of the request, upon giving the prior notice to you.

Cookies, signals and similar technology

The term *cookies* used in this Policy is used to refer to cookies and other similar technology, for example, pixel tags, web beacons, clear GIFs.

As you visit the website of the Data Controller, our aim is to present the content and functionality tailored to your needs. This requires cookies. These are small information elements saved in your Internet browser. They help the Data Controller to recognise you as a previous visitor of the specific website, store your browsing history in the website and adapting the content appropriately. Cookies also help to ensure smooth functioning of websites, allow monitoring the duration and frequency of browsing the website, and collecting statistical data about the number of website visitors. Analysis of such data allows the Data Controller to improve his websites and make them more user-friendly.

When you use your browser to access the content presented by the Data Controller, you can configure your browser to accept all cookies, reject all cookies or request notification when the cookies are downloaded.

Every browser is different; therefore, if you do not know how to change cookie settings, check with its help menu. Your operating system may have additional cookie controls. If you object to the collection of your information by means of cookies, use a simple feature available in most browsers, which allows rejecting the cookies. To learn more about how to manage cookies, please visit <http://www.allaboutcookies.org/manage-cookies/>.

Keep in mind, however, that some services may require cookies, so if you disable them, you will be unable to use all or part of such services.

In addition to the cookies used by the Data Controller, the Data Controller's websites allow certain third parties to set up and access cookies on your computer. In such event, third-party privacy rules apply to the use of cookies.

Please note that social network accounts of the Data Controller are subject to the cookie policy of the appropriate social network.

When collecting and using personal data entrusted to the Data Controller and received from other sources, the Data Controller is guided by the following principles:

- Your personal data are processed in a lawful, fair and transparent manner (principles of lawfulness, fairness and transparency).
- Your personal data are collected for specified, explicit and legitimate purposes and will not subsequently be processed in ways that conflict with such purposes (principle of purpose limitation).
- Your personal data are adequate, appropriate and such that are needed to achieve purposes for which they are processed (principle of data minimisation).
- The processed data are accurate and updated, if necessary (principle of accuracy).
- Your personal data are stored in such form that permits identifying you to the extent this is necessary to achieve purposes for which the data are processed (principle of storage period limitation).
- Your personal data are processed in a way that, through the use of the appropriate technical and organisational measures, adequate protection of such data is ensured, including protection from unauthorised or unlawful processing of data and accidental loss, destruction or damage (principle of integrity and confidentiality).

If you noticed any inadequacies in this Policy, security gaps in the Data Controller's website, or if you have other questions regarding the processing of your personal data, please contact the Data Controller by any of the following means:

Mail: PCB Baltic UAB
Address: Nadruvos 10, LT-06228 Vilnius
Email: sales@pcbbaltic.lt
Telephone: +370 5 2754877

This Policy will be reviewed at least once in two years. In case of any updates to the Policy, you will be informed about changes that we believe to be significant by a notice published on our website. If you log in to or use our content and/or services after such notice is published, it will be deemed that you agree to the new requirements provided for in the updated version.