Privacy Policy

This General Privacy Policy ("Privacy Policy") applies to products and services of Big Dig Data s.r.o. and its affiliates (collectively "we," "us" or "our").

The Controller of your personal data is Big Dig Data s.r.o., which has its principal place of business at Opletalova 85, 252 30 Řevnice, Czech Republic.

1 Privacy Policy Contents

This Privacy Policy describes how we handle and protect your personal data and the choices available to you regarding collection, process, access, and how to update, correct and delete your personal data. Additional information on our personal data practices may be provided in product settings, contractual terms, or notices provided prior to or at the time of data collection.

Please refer to our Products Policy describing specifics of personal data processing within our products and services available on each brand's website (CELUS Plus, Pythia).

2 Personal Data We Process

Personal data ("Personal Data") refers to any information relating to an identified or identifiable natural persons that are our direct customers and, where our customer is a business or similar entity, individuals that are our customer's employees, agents and other representatives. These individuals about whom we collect personal information are referred to as "you" throughout this Privacy Policy.

We may collect data or ask you to provide certain data when you visit and use our websites, products and services. The sources from which we collect Personal Data include:

- Data collected directly from you or your device relating to an identified or identifiable natural person ("Data Subject"), and may include direct identifiers such as name, address, email address, phone number, and online or indirect identifiers such as login account number, login password or IP address;
- If we link other data relating to you with your Personal Data, we will treat that linked data as Personal Data; and

We organize the Personal Data we process into these basic categories: Billing Data, Account Data, and Product Data.

Billing Data includes your name, email address, license information, your billing address and your phone number.

Billing data	What we use it for
Email address	To send you purchase receipts
License key	To identify a specific license for a follow-up actions such as renewal or troubleshooting
License type	To enable features based on the purchased license
Renewability	To check if a given subscription can be renewed
Date of expiry	To check whether an account is valid
Billing address	For invoicing
Phone number	To contact you regarding any issues related to your account

Account Data includes information needed to set up and customize an account, such as your email address and name, and information connected with our services, such as license keys. See below an example of Account Data and what we use it for:

Account data	What we use it for
Email address	To send you communications regarding your license and support
Name	To manage your account and facilitate your login into the service
Subscription renewal date	To tell us until when the account is valid

Product Data includes any information we collect as a result of your sharing of your data with us directly or through third parties. If you want more details about Product Data we process on a product basis, please refer to our Product Policy available on each brand's website (CELUS Plus, Pythia).

3 Why We Process Your Personal Data

We use your Personal Data for the following purposes and on the following grounds:

On the basis of fulfilling our contract with you or entering into a contract with you on your request, in order to:

- Process purchase of our products or services from us, our partners or our trusted third- party service providers' online stores;
- Provision the download, activation, and performance of the product or service;
- Keep our products or services up-to-date, safe and free of errors;
- Verify your identity and entitlement to paid products or services, when you contact us for support or access our services;

- Process your purchase transactions;
- Update you on the status of your orders and licences;
- Manage your subscriptions and user accounts; and
- Provide you with technical and customer support.

On the basis of your consent, in order to:

- Subscribe you to a newsletter.

On the basis of legal obligations, we process your Personal Data when it is necessary for compliance with a legal tax, accounting, anti-money laundering, legal order, or other obligation to which we are subject.

On the basis of our legitimate interest we will use your Personal Data for:

- Communications about possible security, privacy and performance improvements and products that supplement or improve our purchased products and to optimize the content and delivery of this type of communication;
- Product development, research and to implement product features and improvements, as well as product updates;
- Third-party analytics to evaluate and improve the performance and quality of our products, services and websites and to understand usage trends, and analyze user acquisitions, conversions and campaigns;
- Allow interoperability within our applications;
- Secure our systems and applications;
- Allow effective performance of our business by ensuring necessary internal administrative and commercial processes (e.g. finances, controlling, business intelligence, legal & compliance, information security etc.); and
- Establishing, exercising or defending our legal rights.

We have balanced the interests for the above-mentioned processing operations. You have the right to object, on grounds relating to our particular situation, to those processing operations. For more details please see section Your Privacy Rights.

4 Balancing Legitimate Interests

Before relying on our legitimate interests, we balanced them against your interests and made sure they are compelling enough and will not cause any unwarranted harm. With respect to the purposes below, we consider necessary to explain what our interests are in detail.

4.1 Systems, Apps and Network Security

We process Personal Data for network and information security purposes. In line with EU data protection law, organizations have a recognized legitimate interest in collecting and processing Personal Data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security. This primarily covers the ability of a network or of an information system to resist events, attacks or unlawful or malicious actions that could compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, or the security of the related services offered by, or accessible via those networks and systems.

4.2 In-product and Email Messages

We have a legitimate interest for messaging our users about possible security, privacy and performance improvements and products that supplement or improve purchased products.

4.3 New Product Development

We have a legitimate interest to use necessary Personal Data to develop new products or features so that we are able to provide you with state-of-the-art products.

4.4 Third-party Analytics Tools (user acquisition, user interactions)

We have a legitimate interest to use necessary Personal Data for third-party analytics to understand user experience with our products to maintain and enhance functionality, effectiveness, security and reliability of our products and business activities.

5 How We Process Your Personal Data

We do our best to disconnect or remove all direct identifiers from the Personal Data that we use. We continuously monitor for, minimize, disconnect and remove all direct identifiers during the normal performance of the products and services.

5.1 Processing of IP Addresses

For our products, your IP address is processed and stored for safety reasons to allow identification of any potential unauthorised access to your Product Data.

6 How We Disclose Your Personal Data

We only disclose your Personal Data as described below, within our group, with our partners, with service providers that process data on our behalf and with public authorities, as required by applicable law. Processing is only undertaken for the purposes described in this Privacy Policy and the relevant Product Policy sections. If we disclose your Personal Data, we require its recipients to comply with adequate privacy and confidentiality requirements, and security standards.

6.1 Cookies Providers

Our websites use cookies to personalize your experience on our sites, tell us which parts of our websites people have visited, help us measure the effectiveness of campaigns, and give us insights into user interactions and user base as a whole so we can improve our communications and products.

6.2 Cloud Infrastructure Providers

We use cloud storage services to give you the best possible user experience and enhance performance (speed) of the products and services and the level of protection (security) of the data provided to us.

Below, we list these partners and tools and their privacy policies.

Tool (provider)	**Link to Privacy Policy**
Digital Ocean	https://www.digitalocean.com/legal/data-processing-agreement/
	https://www.digitalocean.com/legal/privacy-policy/

6.3 Analytics Tools Providers

We use analytical tools, including third-party analytical tools, which allow us to, among other things, identify potential performance or security issues with our products, improve their stability and function, understand how you use our products, and websites, so that we can optimize and improve your user experience, as well as evaluate and improve our campaigns. We use Product Data for analytics.

While we generally prefer using our own analytical tools, we sometimes need to partner with other parties, which have developed and provide us with their own tools and expertise. Below, we list these partners and tools and their privacy policies.

Tool (provider)	**Type of Analytics**	**Link to Privacy Policy**	**Location**
Google Analytics (Google)	user behaviour	https://support.google.com/analytics/answer/6004245	US, Ireland
		https://policies.google.com/privacy	
		https://support.google.com/analytics/answer/6366371?hl=en&ref_topic=2919631	

Please note that not all of our products use all of these third-party analytics tools. Analytics tools that we use for diagnosing your product are necessary for service provision.

6.4 Public Authorities

In certain instances, it may be necessary for us to disclose your Personal Data to public authorities or as otherwise required by applicable law. No Personal Data will be disclosed to any public authority except in response to:

- A subpoena, warrant or other process issued by a court or other public authority of competent jurisdiction;
- A legal process having the same consequence as a court-issued request for data, in that if we were to refuse to provide such data, it would be in breach of local law, and it or its officers, executives or employees would be subject to liability for failing to honor such legal process;
- Where such disclosure is necessary for us to enforce its legal rights pursuant to applicable law; or
- A request for data with the purpose of identifying and/or preventing credit card fraud.

6.5 Mergers, Acquisitions and Corporate Restructurings

Like any other company, we too go through its own cycle of growth, expansion, streamlining and optimization. Its business decisions and market developments therefore affect its structure. As a result of such transactions, and for maintaining a continued relationship with you, we may transfer your Personal Data to a related affiliate.

If we are involved in a reorganization, merger, acquisition or sale of our assets, your Personal Data may be transferred as part of that transaction. We will notify you of any such deal and outline your choices in that event, when applicable.

6.6 Cross-Border Transfers of Personal Data among Big Dig Data Entities and to Third-Party Vendors

We are a global business that provides its products and services all around the world. In order to reach all of our users and provide all of them with our software, we operate on an infrastructure that spans the globe. The servers that are part of this infrastructure may therefore be located in a country different than the one where you live. In some instances, these may be countries outside of the European Economic Area ("EEA"). Regardless, we provide the same GDPR-level of protection to all Personal Data it processes.

At the same time, when we transfer Personal Data outside of the EEA, we always make sure to put in place appropriate and suitable safeguards, which legally bind the receiving party to adhere to a high level of protection, and to ensure that your data remains safe and secure at all times and that your rights are protected.

Situations where we transfer Personal Data outside of the EEA include provision of our products and services and the provision of support services. Further, an outside-EEA transfer may also occur in case of a merger, acquisition or a restructuring, where the acquirer is located outside of the EEA (see the Mergers, Acquisitions and Restructurings section).

7 How We Protect Your Personal Data

We maintain administrative, technical, and physical safeguards for the protection of your Personal Data.

7.1 Administrative Safeguards

Access to the Personal Data of our users is limited to authorized personnel who have a legitimate need to know based on their job descriptions, for example, employees who provide technical support to end users,

or who service user accounts. In the case of third-party contractors who process personal information on our behalf, similar requirements are imposed. These third parties are contractually bound by confidentiality clauses, even when they leave. Where an individual employee no longer requires access, that individual's credentials are revoked.

7.2 Technical Safeguards

We store your personal information in our database using standard security measures. In addition, we utilize up-to-date firewall protection for an additional layer of security. Third parties who we hire to provide services and who have access to our users' data are required to implement privacy and security practices that we deem adequate.

7.3 Proportionality

We strive to collect no more Personal Data from you than is required by the purpose for which we collect it. This, in turn, helps reduce the total risk of harm should data loss or a breach in security occur: the less data we collect, the smaller the overall risk.

8 How Long We Store Your Personal Data

We will hold your Personal Data on our systems for the following periods:

- For Billing Data, for as long as we have a legal obligation or for our legitimate interests in establishing legal rights;
- For Account Data, for as long as you maintain your account;
- For Product Data, only as long as necessary for the purposes of a particular product or service. Please note that when the provision of services or your license to a product is terminated, processing of Product Data for service provision, in-product messaging and third-party analytics and third-party ads, if applicable, dependent on the product shall cease. Product Data may still be processed and used for development of new features, services and products.

9 Storage of Your Personal Data

The data we collect from you may be stored, with risk-appropriate technical and organizational security measures applied to it, on in-house as well as third-party servers in Germany, as well as anywhere we or our trusted service providers and partners operate. In case we collect data from you on the basis of fulfilling our contract you signed with us, the location where your data is stored and processed is specified in the contract.

In all cases, we follow generally accepted standards and security measures to protect the personal data submitted to us, both during transmission and once we receive it.

10 Your Privacy Rights

You have the following rights regarding the processing of your Personal Data:

- Right to information - Right to receive information about the processing of your Personal Data, prior to processing as well as during the processing, upon request.
- Right of access - Aside from the information about the processing of your Personal Data, you have the right to receive a copy of your Personal Data undergoing processing.
- Right to rectification - We should process accurate Personal Data; if you discover inaccuracy, you have the right to seek rectification of inaccurate Personal Data.
- Right to erasure ("right to be forgotten") - You have the right to erasure of your Personal Data, but only in specific cases stipulated by law, e.g., if there is no legally recognized title on our part for further processing of your Personal Data (incl. protection of Big Dig Data's legitimate interests and rights).
- Right to data portability - The right to receive Personal Data which you have provided and is being processed on the basis of consent or where it is necessary for the purpose of conclusion and performance of a contract, in machine-readable format. This right applies exclusively to Personal Data which processing is carried out by automated means.
- Right to object - Applies to cases of processing carried out in legitimate interest. You have the right to object to such processing, on grounds relating to your particular situation, and we are required to assess the processing in order to ensure compliance with all legally binding rules and applicable regulations. In case of direct marketing, we shall cease processing Personal Data for such purposes after the objection.
- Right to withdraw consent - In the case of processing based on your consent, you can withdraw your consent at any time, by using the same method (if technically possible) you used to provide it to us (the exact method will be described in more detail with each consent when you provide it). The withdrawal of consent shall not affect the lawfulness of processing based on your consent before its withdrawal.
- Right to restriction of processing - You have the right to restriction of processing of your Personal Data if: You are contesting the accuracy of your Personal Data, for a period enabling us to verify the accuracy of your Personal Data; the processing is unlawful and you oppose the erasure of the Personal Data and request the restriction of its use instead; we no longer need the Personal Data for the purposes of the processing, but they are required by you for the establishment, exercise or defence of legal claims; or you have objected to processing of your Personal Data, and there is a pending verification whether our legitimate grounds override your interests.
- Right to contact supervisory authority, court - You may contact and lodge a complaint with the supervisory authority – The Office for Personal Data Protection (Czech: Úřad na ochranu osobních údajů – www.uoou.cz) or your local authority or a relevant court.

The fulfillment of data subject rights listed above will depend on the category of Personal Data and the processing activity. In all cases, we strive to fulfill your request.

We will action your request within one month of receiving a request from you concerning any one of your rights as a Data Subject. Should we be inundated with requests or particularly complicated requests, the time limit may be extended to a maximum of another two months. If we fail to meet these deadlines, we would, of course, prefer that you contact us to resolve the situation informally.

Where requests we receive are manifestly unfounded or excessive, in particular because of their repetitive character, we may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request.

11 Contact Us

To exercise any of your rights, or if you have any other questions or complaints about our use of your Personal Data and its privacy, write our Privacy Team through the most convenient channel below:

We are registered as Big Dig Data s.r.o. and our registered address is Opletalova 85, 252 30 Řevnice, Czech Republic. You can always reach us by email at support@bigdigdata.com. Please type “PRIVACY REQUEST” in the message line of your email so we can have the appropriate member of the Big Dig Data team respond.

If you prefer, you can send paper mail to Big Dig Data s.r.o., Opletalova 85, 252 30 Řevnice, Czech Republic. Be sure to write "Attention: PRIVACY" in the address so we know where to direct your correspondence.

12 Data Protection Officer

As required under the GDPR, we have a data protection officer (DPO) to monitor our compliance with the GDPR, provide advice where requested and cooperate with supervisory authorities. You can contact our data protection officer via support@bigdigdata.com.

13 Changes to this Privacy Policy

We reserve the right to revise or modify this Privacy Policy. In addition, we may update this Privacy Policy to reflect changes to our data practices. If we make any material changes, we will notify you by email (sent to the e-mail address specified in your account) prior to the change becoming effective.