



PRIVACY POLICY

INTECH d.o.o. is committed to protecting and respecting your privacy. This Privacy Policy describes the policies and procedures of INTECH d.o.o. in the gathering, use and disclosure of your data we have collected so far, through publicly accessible sources on the Internet, and with your use of our services, web pages and applications offered by INTECH d.o.o. ("services"). By using the services, you agree to our use of your information in accordance with this Privacy Policy. We will not use or share your personal information with anyone except as described in this Privacy Policy.

This Privacy Policy applies to INTECH d.o.o., therefore, the terms "INTECH", "us", or "ours" refer to INTECH d.o.o., which is the administrator and the entity responsible for the personal data we gather about you.

The data administrator is INTECH d.o.o., Vrhovčeva ulica 10, 1000 Ljubljana, Slovenia. Business unit: Slovenska cesta 54, 1000 Ljubljana.

We may occasionally change this Privacy Policy by publishing an updated version on our website. We encourage you to regularly check this page to stay informed and to make sure that you agree to all the changes. If the Privacy Policy changes significantly, we will inform you if possible via email or by a notification when you sign up, or when you open our app. In order to be able to use our services, you must accept the terms and conditions of this Privacy Policy in its entirety.

1. Legal basis of Privacy Policy

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and on the repealing of Directive 95/46/EC)
- Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 94/07 - official consolidated text) ZVOP-1
- Consumer Protection Act (ZVPot)

1. Gathering information about you

1.1. You can provide us with information by filling in the form on our website, or you can entrust us with your data via telephone or email. This includes the information you provide when registering an account, the process of concluding a contract, reporting problems with the application, providing information for payment, and other interfaces where you provide information or where we gather them from other sources. The personal information you provide may include, but are not limited to, your name and surname, address, email address, IP address, job name, phone number, tax number, transaction account and company information (Company Name; Company Address; Contact Details; Company Tax Number; Iban; Swift; Company Identification Number; Data Set may include other data if involved in the process. In the case of implementation and procedures of the AML policy, the implementation of the **Law on Prevention of Money Laundering and Terrorist Financing**, among other, we check the process of operation and the way of doing business (company plan); Expected Turnover; Certificate of Residence; confirmation that the site is in the ownership and under the control of the person concerned).

1.2. For financial settlements based on transactions, we gather the details of your bank account.

1.3. In order to verify your identity and related information, in accordance with the valid AML policy and the Law on Prevention of Money Laundering and Terrorist Financing, we can provide information about you for the processing and gathering by 3 providers.

Processed data from these providers are received and stored in accordance with the above procedures. We are not required to provide this information.

1.4. When you use our services, we gather information about your transactions, including time, place, transaction amount, type of payment and account holder, IP address and other related information.

1.5. The purpose of using data

The processing of personal data is necessary for the performance of the contract and the fulfillment of legal obligations, and for other purposes as part of the fair use and processing of data for internal and marketing use. We use your personal information only for the purposes for which it was gathered, unless we consider that it can be used for other purposes that is compatible with the original purpose, or if it is contractually and legally required from us. If we would need your personal information for purposes that are incompatible with the original purposes, we shall inform you accordingly and explain the legal basis that allows us to do this. Please note that your personal data may be processed, stored and transmitted without your awareness or consent under the contract, if required or permitted by law.

1.5.1 The purpose of using, collecting and processing your data as set out below in individual services

1. Merchant Applications:
 - a. Verifying the data of the trader and related parties for the purpose of engaging in payment services, implementing a possible contract, assessing the risk and preparing all necessary documents for initiating the joining procedure and opening a merchant account
 - b. Verification and retention of identity documents for the requirements of related services (regulated financial transactions, integration into electronic wallet systems, etc., under the AML 4.1 Directive)
 - c. Retention, transmission and processing of data for the purposes of complying with contractual and other legal provisions
2. PaymentGateway Dashboard:
 - A. Gathering, retention and processing of data for the purpose of fitting metadata for financial transactions and related activities
 - B. Fitting a merchant account with data relevant to processing, reviewing, analytics and reporting in connection with card and other transactions.
 - C. In the case of a merchant account, for managing access to the commercial part of the portal, recording activities and reporting
3. KYCSafe user

Verification and retention of identity documents for the requirements of related services (regulated financial transactions, integration into electronic wallet systems, etc., under the AML 4.1 Directive)

1.5.2. Data gathered:

1. Merchant Applications:
 - Company name, address, tax number, registration number for legal entities and natural persons
 - Contact details (email address and phone number)
 - Registration of the company (extract from the Ajpes business or court register, court)
 - Bank statement for a period of 6 months, whereby individual transactions are visible
 - Business plan of start-up businesses if they do not present bank statements
 - Personal documents (a copy of a passport or identity card) and a residence certificate
 - Ownership of a website's domain insofar as applicable to the company
2. PaymentGateway Dashboard:
 - Name and address of the company
 - Company contact information (email address and phone number)
 - Contact details of the responsible person (email address and phone number)
 - Bank account information
3. KYCSafe user side:
 - Contact details (email address and phone number)
 - Bank statement for a period of 6 months, whereby individual transactions are visible
 - Personal documents (a copy of a passport or identity card)
 - Certificate of residence

Regardless of the data types mentioned, in the case of additional requirements or expanded needs, the data set can be increased to the data that we urgently need to carry out the purpose and which are therefore considered a minimum set of data.

1.5.3. The interfaces in which data are processed and where authorized users access these data

1. KYCSafe ADMIN
2. AUTH DASHBOARD
3. MAILER DASHBOARD
4. PAYMENT GATEWAY
5. MERCHANT APPLICATIONS
6. OTHER ADMINISTRATIVE AND ANALYTIC INTERFACES REQUIRED FOR OPERATION AND REPORTING, INCLUDING AUTOMATED SYSTEMS.

All access to the data is recorded including the purpose of access and the person accessing them.

2. Data processing

2.1. Information we have gathered about you is used to provide our services, and that we can provide you with all relevant information, including evidence on transactions, payout reports, security alerts, and aid messages.

2.3. Information gathered about you can be used to communicate with you about the news and updates of our services, and to notify you about any promotions, initiatives and awards we offer, unless you reject this communication.

You can reject this communication by sending your request for cancellation of consent by email to gdpr@intech.si.

2.4. We can also gather information about cookies and web beacons (see section 7 for further details).

2.5. We may use your information to protect our rights, and to investigate and prevent fraud or other illegal activities, and for any other purpose that would be disclosed in connection with you and that is bound to our services.

3. Use of your personal information

3.1. We can share your information with a member of our group of companies, including subsidiaries, our final holding companies and their subsidiaries, and contracted business partners. This data will be transmitted in order to offer you a comprehensive service in which other companies within our group implement the components of the complete service offered. These other services include customer care, AML Policy implementation, settlement, internal control, etc.

3.2. For marketing and promotion purposes.

3.3. Data may be disclosed if required by third parties which, under our order, perform payment processing or anti-money laundering measures and service providers verification, such as financial institutions, processors, credit card associations and other institutions that form part of the payment and gathering process.

3.4. We can disclose the information gathered about you to third parties in connection with the merger, the sale of company shares or other assets, financing, purchasing, disposing of or canceling all or part of our business.

3.5. We can also disclose the information collected about you,

(i) if disclosure is necessary to comply with applicable law or the relevant arrangements;

(ii) for the enforcement of applicable operating conditions or directives;

(iii) to protect security or to integrate our services; and

(iv) to protect our rights.

3.6. In any case, we will always ensure that your information is gathered, stored, processed or transmitted on a fair-use basis and in connection with the services and in accordance with this Privacy Policy and the applicable data protection provisions.

4. International information provision

4.1. Information gathered about you can be forwarded to members of a group of companies and third parties working with our company, as well as to countries outside the European Economic Area (EEA) or countries for which the European Commission considers that they have a satisfactory data protection. These other countries may not provide the same level of protection for data gathered in the EEA, however, we shall gather, store and use your information at any time in accordance with this Privacy Policy and the General Data Protection Act (GDPR). Intech d.o.o. ensures that it will only share data with those organizations that provide an adequate level of data protection in accordance with applicable data protection laws and that satisfactory contractual agreements are in place between any of these parties.

5. Data protection

5.1. We strive to ensure that the information gathered is safe. We take appropriate measures, including administrative, technical and physical procedures, to protect your information from loss, theft, misuse, unauthorized access, disclosure, alteration and destruction. When logged in to your account, the entire Internet communication is secured with Secure Socket Layer ("SSL") technology ensuring high security with a 128-bit code or higher.

5.2. This high level of security can only be effective when you yourself follow certain security practices of not sharing information about your account and credentials with anyone. If you believe that any of your account credentials have been used, you can change your password at any time on our website or mobile app, however, be sure to always contact Customer Support immediately.

5.3. Unfortunately, the transmission of data over the Internet is not completely secure. Therefore, we can not provide ABSOLUTE security when submitting your information. Any procedure is carried out at your own risk. All data is received, stored and processed in a way that ensures the highest possible level of security and compliance with good business practices, or according to the best of capabilities.

6. Protection of cardholder data

6.1. Intech is responsible for protecting cardholder's data that is processed, transferred, and stored in our systems. To this end, Intech is self-certified according to the Payment Card Industry Data Security Standard (PCI-DSS)). Intech uses the best industry practice to store these sensitive data and to ensure compliance with these requirements. To this end, Intech is annually pursuing continuous care for the preservation of the existing levels of data protection and security in connection with data retention and processing, according to standards in the payment industry.

6.2. For the purpose of anti-money laundering (AML), Intech must keep all transaction data for 10 years after discontinuing a relationship with you as our client. In accordance with the specified request, we store your information - the cardholder's data, in some cases the name, email or phone number used for issuing certificates.

7. Data retention

7.1. We are legally obligated to keep records of collected data for at least ten (10) years after the last transaction or interaction with you. Otherwise, we reserve the right to delete and destroy your gathered data after the expiration of the aforementioned period.

7.2. We store your data in the MS SQL database, properly encrypted and controlled. Data is processed in various tools related to this database and in the Office 365 environment which is, as a by default, subject to the highest standards of control security and privacy, thus allowing for accessibility audit.

7.2. Notwithstanding the above, you have the right to request the deletion of your information. Depending on the services that enable Intech to continue the relationship, for legal purposes, we may need to keep some data for ten (10) years after the request to delete the data or the last transaction or interaction with you. If you request the deletion of your information, we can no longer provide our services.

7.3. You can request the deletion of your information by email at gdpr@intech.si.

8. Cookies and web beacons

8.1. We use a variety of cookies and web beacons within our website and our applications. Cookies are small text files that are stored on your computer, mobile device, or other devices when you browse through our website, or when you use one of our applications or software. Web beacons are small graphic images or other code for web programming that can be included on our website or in our emails.

8.2. Cookies and web beacons can be used for the following purposes:

- (i) to provide service to you as an individual and to adjust the services according to your preferences that you can choose;
- (ii) to facilitate an effective way to operate our website and applications;
- (iii) to monitor site visits or to use applications for static purposes, and to monitor the opinions of users on which sites or functions are useful and which are not;
- (iv) for your identification at check-in and for resetting your password;
- (v) to help us fulfill our supervisory obligations and prevent money laundering and invasion of your account; or
- (vi) to connect with the websites of our groups of companies.

8.3. Some cookies might not apply to Intech services. If you visit a page on our website, including a content added by YouTube or Facebook, for example, the cookies of these websites can be saved to your computer. We do not oversee the spread of third-party cookies, so check out these third-party websites for more information about such cookies and their privacy statements.

8.4. Cookies or web beacons never allow us to access any of your other data on your computer, mobile device, or other devices, except for the information you want to share with us.

8.5. Most browsers accept cookies automatically, but you can change your browser settings by rejecting cookies. Rejected cookies used by our websites, mobile apps or other online software may prevent you from using these pages entirely and may stop them.

8.6. If you do not agree to the use of cookies, turn them off by deleting or modifying cookie settings on your computer, mobile device, or other devices, or stop using the services. For information about deleting or managing cookies, visit www.aboutcookies.org.

9. Connecting with other websites

If you access third-party websites from our website, please note that these websites have their own data protection statements. We do not assume any liability or guarantee for these data protection statements. Check and review these data protection statements before confirming any of your information on these websites.

10. Your rights

We will take all necessary steps to ensure the safe handling of your information in accordance with this Privacy Policy. You have the right to access personal information that we have about you, and the right to repair or delete your information.

If you believe that we are violating your rights, you have the right to appeal to the supervisory authority.

For a better and comprehensive understanding of your rights, check out the following descriptions:

The right of access to your personal information (commonly known as the "request for access to personal information") allows you to receive a copy of the personal information we have about you and to verify that they are processed in a legal manner.

The right to correction of personal information that we have about you allows you to correct incomplete and inaccurate information, whereby we may need to verify the accuracy of the new information you provide to us.

The right to delete your personal information allows you to request the deletion or removal of personal data if there is no legal reason for their further processing. You also have the right to request that we delete or remove your personal information if you have successfully enforced your right to object to the processing (see below), where we may have processed your information illegally or where we had to delete your personal information in accordance with the law.

Please note that we may not always be able to complete your request for deletion for legal reasons that would exist at the time of the request and about which we will notify you.

The right to object to the processing of your personal data, wherein in the course of the processing of the latter we rely on a legitimate interest, and if there is a reason on which you want to object to the processing on such basis and you believe that this affects your fundamental rights and freedoms. You also have the right to object to the processing of your personal data for direct marketing purposes. In some cases, we can prove that we have justified legitimate reasons for processing your data, which supersede your rights and freedoms.

The right to limit the processing of your personal information allows you to request that we temporarily discontinue processing of your personal information in the following cases:

- a) if you want us to determine the accuracy of the data;
- b) if the use of your information is illegal, but you do not want to delete them;
- c) if we do not need your personal information anymore, but you need them to assert, enforce or defend legal claims;
or
- d) if you have filed an objection regarding the use of your information, but we need to verify whether our legitimate grounds for using them outweigh your reasons.

The right to transfer your personal information allows you to request the receipt of your personal information that you have provided us in a structured, widely used and machine-readable form so that we do not hinder you in the process.

If you would like to request a copy of your personal information or to modify, delete or update certain personal information or withdraw consent to process the data, you may do so via the email address gdpr@intech.si.

If you are not satisfied, you have the right to appeal to the relevant data protection authority. Intech will fully participate in any such type of investigation and will make every effort to answer all the questions

11. Withdrawal of agreement

If you want to withdraw your agreement with our Privacy Policy, we need to remind you that in this case we will no longer be able to provide our services, and we may therefore need to terminate all relevant and existing cooperation with you. In addition, we may still need to keep your information for the purpose of legal and regulatory requirements.

12. Applicable law

12.1. This Privacy Policy is governed by the Slovenian law.

12.2. Privacy Policy in the Slovenian version is legally binding. A translation or other language versions of this Privacy Statement are for informational purposes only and are available to users. In the case of contradictions between the English version and any other language version of this Privacy Statement, the Slovenian version prevails.

12.3. This Privacy Statement (including, if applicable, our General Terms and Conditions) specifies the entire agreement, and supersedes all previous agreements, conditions, warranties and/or representations to the fullest extent, if permitted by law.

13. Contact

Feedback or questions regarding the Privacy Policy are welcome and can be addressed to:

Email: gdpr@intech.si, Post: Intech doo, Vrhovčeva ulica 10, 1000 Ljubljana, Slovenia

Date of entry into force: This Privacy Policy was updated on 18 May 2018.