

DATA PROTECTION PRIVACY POLICY

Congress Service Center and Protection of personal data

Congress Service Center hereby declares that in all processing of personal data will fully respect the General Data Protection Regulation (EU) 2016/679. The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas.

The GDPR's primary aim is to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. All personal data acquired by CSC will be processed lawfully and fairly, on the basis of the data subject's consent or another specified basis, conferring rights on the data subject to obtain information about the processing of personal data and to require inaccurate personal data to be rectified, giving the holder of that office responsibility for monitoring and enforcing their provisions.

Congress Service Center takes the protection of personal data very seriously. We treat personal data confidentially in accordance with legislative data protection regulations.

CSC has prepared Data Privacy Statement that should be signed by everyone who is working on behalf of the Company with notice about how CSC collects, uses, and processes your personal information.

We take steps to ensure that the personal information that we collect about you is adequate, relevant, not excessive, and processed for limited purposes.

Contact Details:

Congress Service Center

Vladimir Polezinovski, 22/4 1000 Skopje

R. North Macedonia Email:

office.sk@kscnet.com

www.kscnet.com

T: +389 2 3230 967 | M: +389 78 45 45 04

ISO 9001:2015 ISO 14001:2015 ISO 17100:2015 ISO 20121:2012

Types of personal data we process

Identity data (including name, marital status, nationality photographs, signatures, address, contact details, date of birth, age, passport numbers)

Identification documents (ID, including passports, driving licence, other ID cards, marriage certificates, deed polls, copies of credit card and utility bills, copies of bank statements)

Contact Data includes billing address, delivery address, email address and telephone numbers, as well as details of any additional persons for whom copy correspondence is required.

Correspondence Data includes details of your correspondence with us (including bidding instructions recorded online or over the telephone, and any complaints you have made to our customer services team).

Image data including photographs and video images (from CCTV footage).

Financial Data includes bank account, payment card details, IBAN, SWIFT

Transaction Data includes details about payments to and from you and other details of products and services you have purchased from us, as well as details of your insurance if your property remains at your own risk and details of the property to which our services relate (as well as the nature of these services).

Marketing and Communications Preferences Data includes your preferences in receiving marketing from us and our third parties and your communication preferences.

Lawful basis for processing personal data

CSC takes reasonable and appropriate steps to protect Personal Information against unauthorized access, loss, misuse, disclosure, alteration, destruction and other Processing of Personal Information. These measures take into account the sensitivity of the Processing operation concerned and of the Personal Information concerned, and the risks involved.

CSC will restrict access to Personal Information to those employees, agents and contractors of who haven't a legitimate business need for such access.

Communications and network security controls have been put in place requiring authentication to access computer systems, networks, and other resources. Safeguards are in place to alert CSC when an actual or suspected unauthorized access takes place.

Safeguards in place to protect your personal data

Data collected via direct contact from our employees, is also dealt with in the strictest confidence and is not freely shared. Some of the steps we take to actively safeguard data are:

- ▶ Employees are trained not to share the data with anyone else not directly handling an enquire
- ▶ Financial data to do with the bank accounts are dealt with the strictest confidence
- ▶ Emails, reservations, registrations systems in place have adequate security features in place so that confidentiality is not breached.
- ▶ In case we have to handle personal data in a more public place, we refrain from doing so until we are able to ensure some privacy in the working surroundings.

- ▶ Personal data is not stored for long periods of time- for electronic records automatically expire and in cases where payments are performed only the required supporting documents are securely stored by the relevant financial departments.

Recipients to whom the data may be disclosed

The personal data of the data holder can only be disclosed to responsible internal employees and external clients only upon data holder approval.

To staff management: any internal department involved in carrying out respective business processes.

To public authorities on the basis of statutory regulations (social insurance carriers, tax authorities, health insurance companies); bank institutions (for salary transactions); creditors (in the case of wage / salary garnishment); travel agencies.

Note: CSC does not provide any Personal data to third parties except if such disclosure is necessary in order to protect legitimate interests of CSC or if it is required or permitted by law.

How we process personal data

Congress Service Center activities include event management, translation, interpretation, travel, consultancy and publishing.

Within the context of these activities, personal data is collected, processed, used, and, where applicable, transmitted for the purpose of tenders, marketing needs for publishing or obtaining, implementing, and billing request for services.

How long we keep personal data

Except as otherwise permitted or required by applicable law or regulation, we will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, as required to satisfy any legal, accounting, or reporting obligations, or as necessary to resolve disputes. To determine the appropriate retention period for personal information, we consider our statutory obligations, the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes we process your personal information for, and whether we can achieve those purposes through other means. We specify the retention periods for your personal information in our records management retention schedules.

Under some circumstances we may anonymize your personal information so that it can no longer be associated with you. We reserve the right to use such anonymous and de-identified data for any legitimate business purpose without further notice to you or your consent. Once you are no longer

providing services to us, we will retain and securely destroy your personal data in accordance with our policies and applicable laws and regulations.

Data subject rights

The GDPR gives individuals the following rights:

- ▶ **Right to be informed:** organisations must tell individuals what data of theirs is being collected, how it's being used, how long it will be kept and whether it will be shared with any third parties.
- ▶ **Right of access:** individuals have the right to request a copy of the information that an organisation holds on them.
- ▶ **Right of rectification:** individuals have the right to correct data that is inaccurate or incomplete.
- ▶ **Right to be forgotten:** in certain circumstances, individuals can ask organisations to erase any personal data that is stored on them.
- ▶ **Right of portability:** individuals can request that an organisation transfers any data that it holds on them to another company.
- ▶ **Right to restrict processing:** individuals can request that an organisation limits the way it uses personal data.
- ▶ **Right to object:** individuals have the right to challenge certain types of processing, such as direct marketing.
- ▶ **Rights related to automated decision making, including profiling:** individuals can ask organisations to provide a copy of its automated processing activities if they believe the data is being processed unlawfully. You should also remind individuals that they are free to exercise their rights and explain how they can do this.

You will be provided access to your own Personal Information as required by and in accordance with applicable law. Requests for access, and in general, all data protection related requests, may be made to the local data protection officer.

We may request specific information from you to help us confirm your identity and your right to access, and to provide you with the personal information that we hold about you or make your requested changes. Applicable law may allow or require us to refuse to provide you with access to some or all of the personal information that we hold about you, or we may have destroyed, erased, or made your personal information anonymous in accordance with our record retention obligations and practices. If we cannot provide you with access to your personal information, we will inform you of the reasons why, subject to any legal or regulatory restrictions.