Privacy policy

1. data protection at a glance

General information

The following information provides a simple overview of what happens to your personal data when you visit our website. Personal data is any data that can be used to identify you personally. For detailed information on the subject of data protection, please refer to our data protection declaration listed below this text.

Data collection on our website

Who is responsible for data collection on this website?

Data processing on this website is carried out by the website operator. You can find the operator's contact details in the legal notice of this website.

How do we collect your data?

On the one hand, your data is collected when you provide it to us. This may, for example, be data that you enter in a contact form. Other data is collected automatically by our IT systems when you visit the website. This is primarily technical data (e.g. internet browser, operating system or time of page view). This data is collected automatically as soon as you enter our website.

The collection and processing (including storage, modification, transmission, blocking and deletion) and use of the data is carried out exclusively for the purposes of participant registration and the organization of the event.

Types of data processed:

- Inventory data (e.g., names, addresses).
- Contact data (e.g., e-mail, telephone numbers).
- Content data (e.g., text entries, photographs, videos).
- Usage data (e.g., websites visited, interest in content, access times).
- Meta/communication data (e.g., device information, IP addresses).

What do we use your data for?

For the implementation of the event "GERMAN-KOREAN Aesthetic Face Meeting" on February 22 - 23 2025 in Munich, Germany, participant data will be collected by boeld communication GmbH and passed on exclusively to the scientific organizer - in the case of additional bookings also to the respective organizers and the service providers entrusted with the implementation of this additional booking. If you also register for the newsletter as part of the registration process, your data will also be used to send you mailings/newsletters. This enables us to inform you about our current and future events in the future.

Other data may be used to analyze your user behavior.

Consent
You can withdraw your consent at any time. The following options are available to you for this purpose:
1. by email to datenschutz@bb-mc.com
2. alternatively, you can unsubscribe from the newsletter at the end of each mailing

What rights do you have regarding your data?
You have the right to receive information about the origin, recipient and purpose of your stored personal data free of charge at any time. You also have the right to request the correction, blocking or deletion of this data. You can contact us at any time at the address given in the legal notice if you have any further questions on the subject of data protection. You also have the right to lodge a complaint with the competent supervisory authority.

Analysis tools and tools from third-party providers
When you visit our website, your surfing behavior may be statistically evaluated. This is primarily done using cookies and so-called analysis programs. The analysis of your surfing behavior is usually anonymous; the surfing behavior cannot be traced back to you. You can object to this analysis or prevent it by not using certain tools. Detailed information on this can be found in the following privacy policy.

2 General notes and mandatory information

Data protection

The operators of these pages take the protection of your personal data very seriously. We treat your personal data confidentially and in accordance with the statutory data protection regulations and this privacy policy. When you use this website, various personal data is collected. Personal data is data that can be used to identify you personally. This privacy policy explains what data we collect and what we use it for. It also explains how and for what purpose this is done. We would like to point out that data transmission over the Internet (e.g. when communicating by email) may be subject to security vulnerabilities. Complete protection of data against access by third parties is not possible.

Note on the responsible body

The controller responsible for data processing on this website is
boeld communication GmbH
Reitmorstrasse 25
80538 Munich
Telephone: +49-(0)89-18 90 46-0
E-Mail: contact@bb-mc.com
The controller is the natural or legal person who alone or jointly with others determines the purposes and means of the processing of personal data (e.g. names, e-mail addresses, etc.).

Withdrawal of your consent to data processing
Many data processing operations are only possible with your express consent. You can withdraw your consent at any time. All you need to do is send us an informal email. The legality of the data processing carried out until the revocation remains unaffected by the revocation.
However, participation in the event is not possible without processing your data to the extent described above. An objection will therefore result in your participation in the event being canceled with the agreed contractual consequences.

Right to lodge a complaint with the competent supervisory authority
In the event of breaches of data protection law, the data subject has the right to lodge a complaint with the competent supervisory authority. The competent supervisory authority for data protection issues is the state data protection officer of the federal state in which our company is based. A list of data protection officers and their contact details can be found at the following link: https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html.

Right to data portability
You have the right to have data that we process automatically on the basis of your consent or in fulfillment of a contract handed over to you or to a third party in a common, machine-readable format. If you request the direct transfer of the data to another controller, this will only take place if it is technically feasible.

SSL or TLS encryption
This site uses SSL or TLS encryption for security reasons and to protect the transmission of confidential content, such as orders or inquiries that you send to us as the site operator. You can recognize an encrypted connection by the fact that the address line of the browser changes from "http://" to "https://" and by the lock symbol in your browser line. If SSL or TLS encryption is activated, the data you transmit to us cannot be read by third parties.

Encrypted payment transactions on this website
If there is an obligation to send us your payment data (e.g. account number for direct debit authorization) after the conclusion of a fee-based contract, this data is required for payment processing. Payment transactions via the usual means of payment (Visa/MasterCard, direct debit) are made exclusively via an encrypted SSL or TLS connection. You can recognize an encrypted connection by the fact that the address line of the browser changes from "http://" to "https://" and by the lock symbol in your browser line. With encrypted communication, the payment data you transmit to us cannot be read by third parties.

Information, blocking, deletion
Within the framework of the applicable legal provisions, you have the right to free information about your stored personal data, its origin and recipient and the purpose of the data processing and, if necessary, a right to correction, blocking or deletion of this data at any time. You can contact us at any time at the address given in the legal notice if you have further questions on the subject of personal data.

Objection to advertising emails
We hereby object to the use of contact data published as part of our obligation to provide a legal notice for the purpose of sending unsolicited advertising and information material. The operators of the website expressly reserve the right to take legal action in the event of the unsolicited sending of advertising information, such as spam e-mails.

3. data protection officer
Data protection officer required by law
We have appointed a data protection officer for our company.
Katrin Meyer
Phone: 08171 42 82 766 0
Email: datenschutz@starhead.de

4. data collection on our website
Cookies
Some of the Internet pages use so-called cookies. Cookies do not damage your computer and do not contain viruses. Cookies are used to make our website more user-friendly, effective and secure. Cookies are small text files that are stored on your computer and saved by your browser. Most of the cookies we use are so-called "session cookies". They are automatically deleted at the end of your visit. Other cookies remain stored on your end device until you delete them. These cookies enable us to recognize your browser on your next visit. You can set your browser so that you are informed about the setting of cookies and only allow cookies in individual cases, exclude the acceptance of cookies for certain cases or in general and activate the automatic deletion of cookies when closing the browser. If cookies are deactivated, the functionality of this website may be restricted. Cookies that are required to carry out the electronic communication process or to provide certain functions that you have requested (e.g. shopping cart function) are stored on the basis of Art. 6 para. 1 lit. f GDPR. The website operator has a legitimate interest in the storage of cookies for the technically error-free and optimized provision of its services. Insofar as other cookies (e.g. cookies to analyze your surfing behavior) are stored, these are treated separately in this privacy policy.

Server log files
The provider of the pages automatically collects and stores information in so-called server log files, which your browser automatically transmits to us. These are
Browser type and browser version
Operating system used
Referrer URL
Host name of the accessing computer
Time of the server request
IP address
This data is not merged with other data sources.

The basis for data processing is Art. 6 para. 1 lit. f GDPR, which permits the processing of data for the fulfillment of a contract or pre-contractual measures.

Deletion of data
The data processed by us will be erased or restricted in its processing in accordance with Art. 17 and 18 GDPR. Unless expressly stated in this privacy policy, the data stored by us will be deleted as soon as it is no longer required for its intended purpose and the deletion does not conflict with any statutory retention obligations. If the data is not deleted because it is required for other and legally permissible purposes, its processing will be restricted. This means that the data is blocked and not processed for other purposes. This applies, for example, to data that must be retained for commercial or tax law reasons. According to legal requirements in Germany, data is stored in particular for 6 years in accordance with § 257 para. 1 HGB (commercial books, inventories, opening balance sheets, annual financial statements, commercial letters, accounting documents, etc.) and for 10 years in accordance with § 147 para. 1 AO (books, records, management reports, accounting documents, commercial and business letters, documents relevant for taxation, etc.).

Registration on this website
You can register on our website in order to use additional functions on the site. We use the data entered for this purpose only for the purpose of using the respective offer or service for which you have registered. The mandatory information requested during registration must be provided in full. Otherwise we will reject the registration. In the event of important changes, for example to the scope of the offer or technically necessary changes, we will use the e-mail address provided during registration to inform you in this way.
The data entered during registration is processed on the basis of your consent (Art. 6 para. 1 lit. a GDPR). You can withdraw your consent at any time. All you need to do is send us an informal email. The legality of the data processing that has already taken place remains unaffected by the revocation. The data collected during registration will be stored by us for as long as you are registered on our website and will then be deleted. Statutory retention periods remain unaffected.

Processing of data (customer and contract data)
We collect, process and use personal data only insofar as it is necessary for the establishment, content or modification of the legal relationship (inventory data). This is

done on the basis of Art. 6 para. 1 lit. b GDPR, which permits the processing of data for the fulfillment of a contract or pre-contractual measures. We collect, process and use personal data about the use of our website (usage data) only insofar as this is necessary to enable or charge the user for the use of the service. The customer data collected will be deleted after completion of the order or termination of the business relationship. Statutory retention periods remain unaffected.

Data transfer upon conclusion of a contract for services and digital content
We only transfer personal data to third parties if this is necessary in the context of contract processing, for example to the credit institution responsible for processing payments. Any further transmission of data will not take place or will only take place if you have expressly consented to the transmission. Your data will not be passed on to third parties without your express consent, for example for advertising purposes.
The basis for data processing is Art. 6 para. 1 lit. b GDPR, which permits the processing of data for the fulfillment of a contract or pre-contractual measures.

Administration, financial accounting, office organization, contact management
We process data as part of administrative tasks and the organization of our business, financial accounting and compliance with legal obligations, such as archiving. In doing so, we process the same data that we process as part of the provision of our contractual services. The processing bases are Art. 6 para. 1 lit. c. GDPR, Art. 6 para. 1 lit. f. GDPR. Customers, interested parties, business partners and website visitors are affected by the processing. The purpose and our interest in the processing lies in the administration, financial accounting, office organization, archiving of data, i.e. tasks that serve to maintain our business activities, perform our tasks and provide our services. The deletion of data with regard to contractual services and contractual communication corresponds to the information specified in these processing activities. We disclose or transmit data to the tax authorities, consultants such as tax advisors or auditors as well as other fee offices and payment service providers.

5. newsletter
Newsletter data
If you would like to receive the newsletter offered on the website, we require an e-mail address from you as well as information that allows us to verify that you are the owner of the e-mail address provided and that you agree to receive the newsletter. No further data is collected, or only on a voluntary basis. We use this data exclusively for sending the requested information and do not pass it on to third parties. The data entered in the newsletter registration form is processed exclusively on the basis of your consent (Art. 6 para. 1 lit. a GDPR). You can revoke your consent to the storage of the data, the e-mail address and its use for sending the newsletter at any time, for example via the "Unsubscribe" link in the newsletter. The legality of the data processing operations that have already taken place remains unaffected by the revocation.
The data you provide us with for the purpose of subscribing to the newsletter will be stored by us until you unsubscribe from the newsletter and deleted after you unsubscribe from the newsletter. Data stored by us for other purposes (e.g. e-mail addresses for the member area) remain unaffected by this.

CleverReach

This website uses CleverReach to send newsletters. The provider is CleverReach GmbH & Co. KG, Mühlenstr. 43, 26180 Rastede, Germany. CleverReach is a service with which the newsletter dispatch can be organized and analyzed. The data you enter for the purpose of receiving the newsletter (e.g. e-mail address) is stored on CleverReach's servers in Germany or Ireland. Our newsletters sent with CleverReach enable us to analyze the behavior of newsletter recipients. Among other things, we can analyze how many recipients have opened the newsletter message and how often which link in the newsletter was clicked on. Conversion tracking can also be used to analyze whether a predefined action (e.g. purchase of a product on our website) has taken place after clicking on the link in the newsletter. Further information on data analysis by CleverReach newsletters can be found at https://www.cleverreach.com/de/funktionen/reporting-und-tracking/.

Data processing takes place on the basis of your consent (Art. 6 para. 1 lit. a GDPR). You can revoke this consent at any time by unsubscribing from the newsletter. The legality of the data processing operations that have already taken place remains unaffected by the revocation. If you do not want CleverReach to analyze your data, you must unsubscribe from the newsletter. We provide a link for this purpose in every newsletter message. You can also unsubscribe from the newsletter directly on the website. The data you provide us with for the purpose of subscribing to the newsletter will be stored by us until you unsubscribe from the newsletter and deleted from both our servers and CleverReach's servers after you unsubscribe from the newsletter. Data stored by us for other purposes (e.g. e-mail addresses for the member area) remain unaffected by this. You can find more details in CleverReach's privacy policy at https://www.cleverreach.com/de/datenschutz/.

Conclusion of a contract for commissioned data processing

We have concluded a contract with CleverReach for commissioned data processing and fully implement the strict requirements of the German data protection authorities when using CleverReach.

6. payment provider

PayPal

We offer payment via PayPal on our website. The provider of this payment service is PayPal (Europe) S.à.r.l. et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxembourg (hereinafter referred to as "PayPal").

If you select payment via PayPal, the payment data you enter will be transmitted to PayPal. The transmission of your data to PayPal is based on Art. 6 para. 1 lit. a GDPR (consent) and Art. 6 para. 1 lit. b GDPR (processing for the performance of a contract). You have the option to withdraw your consent to data processing at any time. A revocation does not affect the effectiveness of data processing operations in the past.

Instant bank transfer

On our website we offer payment via "Sofortüberweisung". The provider of this payment service is Sofort GmbH, Theresienhöhe 12, 80339 Munich (hereinafter referred to as "Sofort GmbH"). With the help of the "Sofortüberweisung" procedure, we receive

a payment confirmation from Sofort GmbH in real time and can immediately begin to fulfill our obligations. If you have opted for the "Sofortüberweisung" payment method, you transmit the PIN and a valid TAN to Sofort GmbH, with which it can log into your online banking account. After logging in, Sofort GmbH automatically checks your account balance and carries out the transfer to us using the TAN you have transmitted. It then immediately sends us a transaction confirmation. After logging in, your turnover, the credit limit of the overdraft facility and the existence of other accounts and their balances are also checked automatically. In addition to the PIN and the TAN, the payment data entered by you and your personal data are also transmitted to Sofort GmbH. Your personal data includes your first and last name, address, telephone number(s), email address, IP address and any other data required for payment processing. The transmission of this data is necessary to establish your identity beyond doubt and to prevent attempts at fraud. The transmission of your data to Sofort GmbH is based on Art. 6 para. 1 lit. a GDPR (consent) and Art. 6 para. 1 lit. b GDPR (processing for the performance of a contract). You have the option of withdrawing your consent to data processing at any time. A revocation does not affect the effectiveness of data processing operations in the past. Details on payment by instant bank transfer can be found in the following links:
https://www.sofort.de/datenschutz.html and https://www.klarna.com/sofort/.

Credit card payment | ingenico | ogone
1. processing of personal data
1.1 Description of the processing
The processing carried out by Ingenico ECS under the Merchant Agreement has the following characteristics:

(a) The Dealer is the controller or co-controller of the processing within the meaning of data protection law (General Data Protection Regulation - Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, as amended or replaced from time to time, and up to and including May 24, 2018, Directive 95/46/EC of October 24, 1995 and its local implementation).

b) Ingenico ECS acts as processor of the Merchant and in accordance with its instructions. Ingenico ECS is not the controller for this processing, except for the specific services for which Ingenico ECS or an affiliated company within the meaning of §§15 et seq. AktG is expressly designated as the controller in the dealer agreement. If Swiss or Austrian law applies, the comparable provisions of the applicable law shall apply.

c) The merchant has chosen the Ingenico Service as the best solution to process personal data for the purposes described below.

d) The purpose of the processing as defined by the Merchant is the processing of transaction-related data and any ancillary or related activities necessary for the processing of payment data. Within the limits described above, the processing

consists of collecting, aggregating, comparing, encrypting, decrypting, organizing, verifying, analyzing, controlling, registering, calculating, reproducing, extending, copying, duplicating and forwarding personal data to the persons involved in the processing of the transactions using the Ingenico ECS e-commerce platform and the tools connected to it via network connections and standard protocols.

e) The personal data that are the subject of processing are personal data that have been collected and processed during the processing of the transactions.

f) The personal data is stored for a period specified in the service description. The period is calculated in calendar days from the date of the transaction. If regulations, laws or contractual provisions do not require Ingenico ECS to retain the personal data, Ingenico ECS will delete or anonymize the personal data at the end of this period. Without prejudice to the backup copies made by Ingenico ECS and insofar as the e-commerce platform of Ingenico ECS permits, the merchant may shorten this retention period. The merchant assumes responsibility for the chosen period. The service description may provide for other modalities for the storage of personal data and their retention period.

1.2 Obligations of Ingenico ECS

As part of its PCI DSS-certified organization, Ingenico ECS implements appropriate technical and organizational measures in its area of expertise to ensure that processing complies with the requirements of data protection law as defined in section 13.1 and guarantees the protection of data subjects.

In its capacity as processor, Ingenico ECS undertakes to

a) to process the personal data only on the instructions of the Merchant, including with regard to the transfer of personal data to a third country or an international organization, whereby the modalities of the Ingenico Service described in the Merchant Agreement shall constitute the instructions of the Merchant;

b) ensure that the persons authorized to process the personal data on its staff or on the staff of its processors have committed themselves to confidentiality or are subject to an appropriate legal obligation of confidentiality;

c) taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk;

d) take steps to ensure that natural persons under the authority of Ingenico ECS who have access to personal data do not process it except on instructions from the merchant, unless required to do so by law, regulation or a judicial or administrative authority;

e) in view of the nature of the processing, assist the Merchant, where possible, with appropriate technical and organizational measures to comply with its obligation to respond to requests to exercise the rights of the data subject in accordance with data protection law as defined in Section 13.1.

If a data subject's requests are manifestly unfounded or excessive, in particular if they are made repeatedly, Ingenico ECS may
e1. require the Merchant to pay a reasonable fee, taking into account the administrative costs of informing or notifying or implementing the requested measure, or
e2. refuse to act on the request;

f) taking into account the nature of the processing and the information available to Ingenico ECS, assist the Merchant in complying with the obligations set out in Articles 32 to 36 of the General Data Protection Regulation (Regulation (EU) 2016/679);

g) to assist the Merchant to comply with its reporting obligations under data protection law as defined in section 1.1, which for Ingenico ECS means

g1. In the event of a personal data breach under the Merchant Agreement by Ingenico ECS or any of its subcontractors which may result in a risk to the rights and freedoms of natural persons, Ingenico ECS shall notify the Merchant of such breach without undue delay after becoming aware of it, so that the Merchant may notify the competent supervisory authority, if appropriate.
g2. The notification by Ingenico ECS pursuant to paragraph g1. shall contain at least the following information:
g2.1 a description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, the categories and approximate number of personal data records concerned;
g2.2 a description of the measures taken or proposed to be taken by Ingenico ECS to address the Personal Data Breach and, where appropriate, measures to mitigate its possible adverse effects.
If and to the extent the information cannot be provided at the same time, Ingenico ECS may provide such information in stages without undue further delay.
g3. In the event of a personal data breach that does not fall into the category referred to in sub-paragraph g1. above, Ingenico ECS shall notify the Merchant of such breach without undue delay after having become aware of it;

h) at the Merchant's option and unless a law, regulation or judicial or administrative authority requires the retention of the Personal Data, either delete or return all Personal Data after termination of the Contract or the end of the retention period and destroy all existing copies, except for the backup copies and the Personal Data stored in the log files;

i) to provide the trader with all information necessary to demonstrate compliance with the obligations set out in this Article and to facilitate and contribute to audits, including inspections, carried out by the trader or another auditor appointed by the trader.

(i) provide the trader with all information necessary to demonstrate compliance with the obligations laid down in this Article and facilitate and contribute to audits, including inspections, carried out by the trader or another auditor mandated by the trader.

The following principles shall apply during an audit: Dealer shall not request more than one (1) audit per year, unless Ingenico ECS seriously neglects its obligations, in which case Dealer may request an additional audit. To conduct an audit, the Merchant shall notify Ingenico ECS by registered letter with acknowledgment of receipt at least six (6) weeks prior to the date of the scheduled audit and enclose a detailed audit plan with this notification. If an audit takes place due to serious misconduct by Ingenico ECS, the Dealer shall inform Ingenico ECS thereof forty-eight (48) hours in advance. The following principles shall apply in all circumstances: 1. the benchmark applicable to the audit shall be the PCI reference applicable to the Ingenico Service. In this context, it is expressly agreed that audits shall not include: any financial or personal data not relating to the Merchant, any information the disclosure of which could compromise the system and/or data security of Ingenico ECS (in which case Ingenico ECS shall justify its refusal on the basis of legitimate interests, e.g. confidentiality or security

reasons) or other Ingenico ECS clients, the source code of Ingenico programs or other tools used by Ingenico ECS. 2. all costs of the audit, including the internal costs of Ingenico ECS, shall be borne by the Dealer. Ingenico ECS will invoice the Dealer for all costs of the audit, including the working days of Ingenico ECS employees, whose working days will be charged at the rate of EUR 1,400.00 per day. (3) The duration of the audit shall not exceed three (3) working days. 4. the auditor may not make complete or partial copies of documents, files, data or information, nor may he take photographs, digitize information, make audio, video or computer recordings or request that these elements be made available or sent to him in full or in part. However, Ingenico ECS may present sensitive documents in a secure room (black room). 5. any natural person acting as an inspector may only be admitted to an Ingenico ECS site or one of its subcontractors once the merchant has confirmed his identity. Regardless of whether auditors are employed by the Dealer or by an external auditing company, the Dealer must ensure the integrity of the auditors employed. The Dealer warrants to Ingenico ECS that the auditor will comply with the confidentiality obligation mentioned in the Dealer Agreement. 6. 6. the audit must take place during the normal office hours of Ingenico ECS and will be carried out in such a way that neither the provision of the Ingenico service nor other activities of Ingenico ECS, which it provides for its other clients, are disturbed; these will in any case take precedence over the performance of the audit. Ingenico ECS may interrupt the audit at any time if the provision of the Ingenico Service requires that the resources and means used for the audit are made available for other purposes;

j) inform the Merchant immediately if Ingenico ECS is of the opinion that an instruction from the Merchant constitutes a breach of data protection law as defined in clause 1.1.

1.3 Subcontractors

Ingenico ECS may engage other processors (hereinafter "Sub-Processors") to carry out certain processing activities on behalf of the Merchant or to replace an existing Sub-Processor, provided that it informs the Merchant ninety (90) days in advance and allows the Merchant to assess the intended change and, in case of objections, to terminate the Merchant Agreement in accordance with the following modalities. The Dealer shall have a period of thirty (30) days from the notification by Ingenico ECS to grant or refuse its approval. Ingenico ECS offers a shared service. Therefore, if the Merchant refuses to authorize the use of another sub-processor or the replacement of an existing sub-processor, the Merchant Agreement shall be terminated with sixty (60) days' notice from the notification of refusal of authorization, unless the parties agree on the engagement of another sub-processor. Termination of the Merchant Agreement shall not entail any termination-related additional costs for either party. At the end of the sixty (60) day period, the merchant shall refrain from further use of the Ingenico Service. If the merchant does not respond within the above-mentioned period of thirty (30) days, the authorization shall be deemed to have been granted.

If Ingenico ECS uses the services of a sub-processor to carry out certain processing activities on behalf of the Merchant, the same data protection obligations as in this

Merchant Agreement shall be imposed on such sub-processor by way of a contract or other legal instrument, in particular providing sufficient guarantees that the appropriate technical and organizational measures are implemented in such a way that the processing is carried out in accordance with data protection law as defined in clause 13.1. If the sub-processor fails to comply with its data protection obligations, Ingenico ECS shall be liable to the Merchant for compliance with the obligations of that sub-processor.

In an emergency, as described below, the merchant authorizes Ingenico ECS to engage a sub-processor or to replace an existing sub-processor with immediate effect. In this case, Ingenico ECS shall inform the Merchant as soon as possible about the involvement of the sub-processor or the replacement of an existing sub-processor. The merchant has a period of thirty (30) days from the notification by Ingenico ECS to grant or refuse its authorization. Ingenico ECS offers a shared service. Therefore, if the Merchant refuses to authorize the engagement of an additional sub-processor or the replacement of an existing sub-processor, the Merchant Agreement shall be terminated with sixty (60) days' notice from the notification of the refusal of authorization, unless the parties agree on the engagement of another processor. Termination of the Merchant Agreement shall not entail any termination-related additional costs for either party. At the end of the sixty (60) day period, the merchant shall refrain from further use of the Ingenico Service. If the Merchant fails to respond within the above thirty (30) day period, the authorization shall be deemed to have been granted. An emergency is any event that makes the provision of the Ingenico Service excessively difficult from a reasonable or commercial point of view.

1.4 Obligations of the merchant

The Merchant undertakes to comply with its obligations under data protection law as defined in clause 13.1.

1.5 Transmission of data

1.5.1 Transmission on the instructions of the merchant

If Ingenico ECS or its sub-processors process personal data in the performance of the Merchant Agreement, the Merchant confirms, accepts and warrants the lawfulness of the communication of all personal data by Ingenico ECS or its sub-processors to third parties, including payment service providers, whose cooperation is essential for the proper performance of the Merchant Agreement and/or the execution of the Merchant's instructions. This may also involve the transfer of personal data to a country outside the European Economic Area that does not offer an adequate level of protection. In this case, the Merchant shall ensure that Ingenico ECS or its sub-processors, as processors acting on behalf of the Merchant, can carry out such transfers of personal data in accordance with applicable laws and regulations (including but not limited to ensuring that the transfer is carried out in a lawful manner).

1.5.2 Transfer to a sub-processor

Should the use of one or more sub-processors on Ingenico ECS's own initiative require the transfer of personal data to a country outside the European Economic Area that does not provide an adequate level of protection, Ingenico ECS and its sub-processors must ensure that the provisions of the General Data Protection Regulation (Regulation (EU) 2016/679) are complied with.

As a result, the merchant's authorization is required if Ingenico ECS is required to transfer personal data to a country outside the European Economic Area that does not have an adequate level of protection in the context of the performance of the merchant agreement.

Ingenico ECS shall notify the Merchant ninety (90) days in advance. The Merchant has a period of thirty (30) days from the notification by Ingenico ECS to grant or deny its authorization. Ingenico ECS offers a shared service. Therefore, if the Merchant refuses to authorize the transmission described above, the Merchant Agreement will be terminated with a notice period of sixty (60) days from the notification of refusal of authorization. Termination of the Merchant Agreement shall not entail any additional termination-related costs for either party. From the end of the sixty (60) day period, the merchant shall refrain from further use of the Ingenico Service. If the merchant does not respond within the aforementioned period of thirty (30) days, the authorization shall be deemed to have been granted.

1.6 Requests from law enforcement authorities and other judicial or administrative authorities

The transfer of personal data of any kind from Ingenico ECS to law enforcement authorities and other judicial or administrative authorities, if such an authority requests such a transfer, will only take place if the merchant instructs Ingenico ECS to do so, unless Ingenico ECS is legally obliged to,

1. to provide such information to law enforcement authorities and other judicial or administrative authorities, and 2. without informing the Merchant. In these circumstances, Ingenico ECS will provide the information to law enforcement authorities and other judicial or administrative authorities without having obtained the

Merchant's authorization and without informing the Merchant of this processing of personal data.

1.7 Processing of personal data as controller

If a party processes personal data as a controller, that party shall ensure that data protection law as defined in clause 13.1 is respected. For example, this party shall ensure that the data subjects are informed about the processing and that the rights of the data subjects are respected.

2. compliance with security standards:

Ingenico e-Commerce Solution SPRL, as a PCI DSS certified service provider, is committed to a comprehensive data security standard, which is met through the use of state-of-the-art technologies and experienced specialists. The certification will be maintained during the term of this Merchant Agreement and its renewals. Subject to the provisions of clause 8, Ingenico ECS, through its subcontractor Ingenico e-Commerce Solutions SPRL, is responsible for the security of the Cardholder Data that Ingenico e-Commerce Solutions SPRL holds or otherwise stores, processes or transmits in the name and on behalf of the Merchant. The nature of Ingenico ECS's e-commerce platform as Software as a Service (SaaS) implies that neither Ingenico e-Commerce Solutions SPRL nor Ingenico ECS can influence the security of the merchant's own cardholder data environment.

The extent to which the merchant is obliged to independently comply with the relevant regulations must be clarified with the payment service provider.