HypoVereinsbank Member of UniCredit

TERMS AND CONDITIONS FOR THE CORPORATE PORTAL

valid from 01. May 2026

1. Range of Services

1.1. Corporate Portal, applications, Communication Suite

The Corporate Portal is the Bank's digital access channel for corporate customers (the "Customer"). The Customer may conduct banking transactions digitally via the Corporate Portal. For this purpose, the Bank provides various applications (see Clause 7). In addition, the Corporate Portal enables secure digital communication between the Bank and the Customer via the Communication Suite (see Clause 8).

1.2. Web-based access

Access to the Corporate Portal is provided via the website made available by the Bank.

1.3. Use as an entrepreneur

The Customer undertakes to use the Corporate Portal exclusively in the course of a commercial or self-employed activity within the meaning of section 14 German Civil Code (BGB) or as a legal entity under private or public law (including foundations). Use as a consumer within the meaning of section 13 German Civil Code BGB is excluded

1.4. Customer's obligation to use

The Customer is obliged to use the Corporate Portal, its applications and the Communication Suite – as far as technically possible and taking into account the interests of both parties – for the independent digital processing of its banking transactions.

2. Customer and Users

2.1. Authorisation of Users

Access to the Corporate Portal is granted only to Users to whom the Customer has granted a corresponding power of attorney. "Users" are:

(1) the Customer itself, provided that the Customer is a natural person,

(2) natural persons having statutory power of representation to represent the Customer (e.g. managing directors) as well as natural persons having a power of attorney (e.g. holder of a general commercial power of representation (Prokuristen)); and

(3) natural persons whom the Customer has authorised accordingly by designating them as Users.

Each User shall act in the name and on behalf of the Customer.

2.2. External power of attorney

By assigning a user role to a natural person, either by the Customer itself or by the Bank acting on behalf of the Customer, the Customer grants such User an external power of attorney (Außenvollmacht) vis à vis the Bank. Such external power of attorney shall apply in addition to any other statutory power of representation or any power of attorney. **Accordingly, the external power of attorney granted to a User shall be independent of whether and to what extent any other power of representation continues to exist. This shall also apply where such other power of representation, or its termination, is registered in a public register** (e.g. as a personally liable partner with authority to represent, as a corporate body of a legal entity or as a holder of a general commercial power of representation (Prokurist)).

Users act within the Corporate Portal exclusively on the basis of the external power of attorney granted to them. This shall also apply to Users holding the role "PoR" (see Clause 2.1. (2)).

2.3. Initialisation of Users

A user only gets access to the Corporate Portal when the Bank has initialised such User. As part of the initialisation process, the Bank assigns individual authentication elements to the User, which the User shall use for future authentication within the Corporate Portal.

Initialisation is subject to the prior identification of the User in accordance with legal requirements.

2.4. User in applications

The use of some applications (see section 7) is only permitted if the User is authorised for the application or the banking transaction that is carried out with the application. The Customer determines the scope of the power of attorney. The Bank generally provides for a standardised scope of power of attorney or standardised user roles for this purpose.
The User can only use the Corporate Portal within the scope of the power of attorney granted to him.

2.5. Users in the Communication Suite; power of attorney to receive documents

An initialised User is given access to the Corporate Portal and may automatically use the Communication Suite for two-way communication with the Bank (see Clause 8). By designating a User, the Customer at the same time grants such User comprehensive power to receive, on behalf of the Customer, all notifications and documents of the Bank relating to the business relationship with the Customer (see Clause 8.3).

Such power of attorney shall be independent of the scope and continued existence of any power of representation granted to the User for applications pursuant to Clause 2.2. Each User shall be individually authorised to receive documents, even if any power of attorney granted to such User for applications is limited to joint representation.

2.6. Customer's obligations with regard to its Users

The Customer must ensure that

- all Users authorised by the Customer comply with these Terms and Conditions, in particular the duties of care pursuant to Clause 4 and the notification and information obligations pursuant to Clause 5;
- personal data of a User is disclosed to the Bank only with the prior consent of the respective User;
- the User data stored in the Corporate Portal is updated without undue delay where necessary;
- Users provide the data required by the Bank concerning the User and/or the Customer and update such data where necessary. The Bank shall request such data where it is required by law or for the proper use of the Corporate Portal and its applications (e.g. provision of an email address for User notifications);
- at least one User is initialised for the Customer's Corporate Portal at all times; and
- all Users are provided with the Bank's applicable data protection notices, which are available at www.hvb.de/eu-dsgvo-hinweise.

2.7. Termination of User status in the Corporate Portal or in applications

The power of attorney granted to a User shall remain in effect until revoked by the Customer either vis-à-vis the Bank or vis-à-vis the User. Wherever possible, such revocation should be effected by self-administration through withdrawal of the User status in the Corporate Portal. Alternatively, revocation vis-à-vis the Bank should, for evidentiary purposes, be made if possible in text form.

If the Customer revokes the power of attorney vis à vis the User, the Customer must inform the Bank thereof without undue delay and, for evidentiary purposes, if possible in text form. In such case, the User's power of attorney shall only terminate upon receipt of such information by the Bank (section 170 BGB), unless the Bank is aware or should have been aware of the termination of the power of attorney (section 173 BGB).

The Customer is also obliged to notify the Bank of the revocation

of a power of attorney even if the User has power to represent the Customer on another legal basis which is registered in a public register and whose termination or modification is registered therein. This notification obligation shall therefore also apply to Users pursuant to Clause 2.1. (2).

The Customer must notify the Bank of the scope of the revocation, i.e. whether it relates to use of the Corporate Portal and all of its applications or only to individual applications. In the case of a self administered revocation, the Customer must ensure that the User status is withdrawn for all relevant applications.

If the Customer has also granted the User a separate power of attorney outside the Corporate Portal, such other power of attorney must be expressly and separately revoked vis à vis the Bank.

2.8. Technical Participants

In individual applications, the Customer may use "Technical Participants". At the Customer's request, the Bank shall set up Technical Participants for the Customer with a defined functional scope.

A Technical Participant is a user account without personal reference which is used for the execution of automated processes, access via technical interfaces (e.g. APIs, machine-to-machine communication) or system integration. The Customer may use a Technical Participant exclusively within the functional scope agreed with the Bank.

3. Access and Authentication

3.1. Access to the Corporate Portal

Access to the Corporate Portal, its applications (see Clause 7) and the Communication Suite (see Clause 8) shall be granted to a User only if

- the User has authenticated itself using the information required by the Bank (e.g. the User's Portal ID) and the authentication elements (see Clauses 3.2. and 3.3.) and
- no suspension of use applies (see Clauses 6).

3.2. Authentication

Authentication means the verification of the User's identity. Authentication is carried out by using the agreed authentication elements.

3.3. Authentication elements are:

- knowledge elements, e.g. a personal identification number (PIN); or
- possession elements, e.g. a device for generating or receiving single-use transaction numbers (TANs), such as a photo-TAN device or a mobile device; or
- inherence elements, i.e. biometric characteristics, e.g. fingerprint or facial recognition.

Authentication is performed by the User transmitting the knowledge element as well as proof of the possession element and/or inherence element to the Bank in accordance with the Bank's specifications.

4. Duties of care of the Customer and, accordingly, of the Users

4.1. Protection of authentication elements

The User is obliged to take all reasonable measures to protect its authentication elements (see Clause 3.3) against unauthorised access. Failing to do so may result in the risk of misuse or other unauthorised use of the Corporate Portal, which may cause damage.

4.2. Examples of protective measures to be taken by the User

For the purpose of protecting the authentication elements, the User must in particular observe the following:

(a) **Knowledge elements** must be kept confidential. In particular, they must not be disclosed orally or in writing and must not be stored electronically in an unsecured manner.

(b) **Possession elements** must be protected against misuse. In particular,

- any activation code provided by the Bank for possession elements must be kept securely and protected from access by third parties in order to prevent unauthorised activation;
- it must be ensured that unauthorised persons do not obtain access to the User's mobile device;
- unauthorised persons must be prevented from using the application for the Corporate Portal itself or an application used for authentication for the Corporate Portal that is installed on the mobile device;
- a physical possession element, such as a photo-TAN device, must at all times remain under the sole control of the authorised User and be stored in such a manner that no other person can use it to generate authentication elements; use by several persons is permitted only if each User activates exclusively its own personalised access on the device;
- evidence of the possession element (e.g. TANs) must not be disclosed either orally or in writing; and,
- the application for the Corporate Portal as well as a physical possession element, such as a photo-TAN device, must be deactivated prior to transfer or disposal of the respective device or disposed of in such a way that use by unauthorised third parties is excluded.

(c) **Inherence elements** (e.g. fingerprints) may be used on a mobile device for authentication in the Corporate Portal only if no inherence elements of other persons are stored on such device. If such elements are stored, a knowledge element (e.g. a PIN) must be used instead.

4.3. Security notices of the Bank

The User is obliged to observe the security notices published by the Bank, in particular those relating to common fraud related risks and methods of attack.

4.4. Exam of transaction data

If the Bank displays to the User the transaction data received by the Bank (e.g. amount, IBAN of the payee), the User is obliged to carefully verify, prior to confirmation, that the displayed data correspond to the data intended for the transaction.

If any discrepancies are identified, the User must immediately terminate the process and notify the Bank without undue delay of the suspicion of misuse.

5. Notification and information obligations of the Customer and, accordingly, of the Users

5.1. Blocking notification to the Bank

The User must notify the Bank without undue delay (blocking notification) if the User

- becomes aware of the loss or theft of a possession element (e.g. a mobile device);
- becomes aware of any unauthorised use of an authentication element; or
- has reason to suspect an unauthorised or fraudulent use of an authentication element.

5.2. Notification to the police
The User is obliged to report any theft or misuse of an authentication element to the police without undue delay.

5.3. Obligation to inform in the event of misuse
The User is obliged to inform the Bank without undue delay upon becoming aware of any unauthorised or incorrectly executed transaction.

6. Suspension of use

6.1. Suspension at the customer's request
At the Customer's request, in particular in the event of a blocking notification pursuant to Clause 5.1, the Bank shall suspend

- the Customer's access or the access of the relevant User to the Corporate Portal; or
- the authentication elements of the relevant User for access to the Corporate Portal.

6.2. Suspension at the Bank's initiative
The Bank is entitled to suspend the Customer's access and/or the access of one or more Users to the Customer's Corporate Portal if

- the Bank is entitled to terminate the Corporate Portal agreement or an agreement relating to an application on the Corporate Portal for good cause;
- objective reasons relating to the security of a User's authentication elements so justify; or
- there is suspicion of unauthorised or fraudulent use of a User's authentication elements.

For security reasons, the Bank is generally entitled to suspend the Customer's access and, accordingly, the access of all Users of the Customer. The Customer shall be informed of the suspension and the material reasons for it, where possible prior to, but at the latest without undue delay after, the suspension has been implemented. The provision of reasons may be omitted if doing so would cause the Bank to breach statutory obligations.

6.3. Automatic suspension of an authentication element
The Bank is entitled to suspend access to the Corporate Portal if the knowledge element required for access is entered incorrectly several times consecutively.

6.4. Lifting of the suspension
For security reasons, the Bank shall generally re initialise the User or Users affected by a suspension (see Clause 2.3) in order to prevent any misuse of the previously used authentication elements. The Customer and/or the affected User shall be informed thereof without undue delay.

7. Applications on the Corporate Portal

7.1. Digital processing of banking transactions
The Customer may use the applications provided by the Bank within the Corporate Portal to conduct banking transactions in digital form. Some applications are subject to fees. The Bank intends to continuously expand the range of applications.

7.2. Separate agreements for applications
Depending on the Customer's intended use of the Corporate Portal, it may be necessary, in addition to this Agreement, to enter into a separate agreement for the respective application, to agree on a fee for such application and/or to authorise Users for the application.

In the event of any inconsistencies between these Terms and Conditions and a separate agreement, the provisions of the separate agreement shall prevail.

In addition to Clause 2.6, the Customer is obliged to ensure that its Users also comply with the provisions of the separate agreement.

Upon termination of the Agreement, the agreements relating to applications shall also terminate simultaneously. Otherwise, the separately concluded agreements relating to applications shall be independent and legally separate from one another and from the Agreement.

7.3. Booking account for fees
The Bank is entitled to debit any agreed fees for applications to the booking account agreed for this purpose. If such account is closed, the Customer must notify the Bank of a new booking account without undue delay. If no such notification is provided, the Bank is entitled to debit another booking account of the Customer at its discretion.

7.4. Submission of orders
If the Bank specifies technical or substantive requirements for certain banking transactions, in particular for Customer orders (e.g. entry of specific data or provision of an authentication element), the Customer must comply with such requirements. The Bank is entitled to amend such requirements at any time.

7.5. Processing of orders
Orders shall be processed by the Bank in accordance with the legal and contractual provisions applicable to the respective type of order and within the proper operational procedures.

7.6. Digital delivery within applications
The Bank is entitled to deliver notifications and documents relating to the Customer via the Communication Suite (see Clause 8) or directly within the relevant application (e.g. confirmation of a completed banking transaction). The Customer is obliged to regularly check the respective application for the receipt of notifications and documents from the Bank.

In certain applications, the User may configure a separate notification (e.g. by email) regarding the availability of new documents (notification function). Such notification is sent unencrypted.

The provisions of Clause 8 apply mutatis mutandis to digital delivery within applications. By way of derogation from Clause 8.6., documents for which no notification is sent shall be deemed to have been received once they have been made available in retrievable and storable form and the User could have taken note of them under ordinary circumstances.

7.7. Multibank functionality
In certain applications, the Bank provides the Customer with a multibank functionality. By means of such multibank functionality, the Customer may use a business relationship maintained with another bank or other financial service provider (third-party institution) within the technical environment of the Corporate Portal. The use of the multibank functionality requires a technical connection to the respective third-party institution, which is established and maintained by the Customer at its own responsibility.

The scope of the functionality depends both on the multibank functionality provided in the relevant application and on the agreements entered into by the Customer with the third-party institution.

In particular, the Customer may, via the multibank functionality

- view and manage data to which it has access at the third-party institution;
- transfer files to or from the third-party institution and
- access payment accounts held with the third-party institution and conduct payment transactions via such accounts.

Where the Customer uses a multibank functionality, the Customer shall be solely responsible for the establishment and maintenance of the access channel to the third-party institution as well as for the management of the data accessible to it there. The Bank shall not obtain knowledge of the identity of the third-party institution or of the content, nature or scope of the data transmitted or managed via the multibank functionality, unless the Customer exceptionally grants the Bank access to such data (e.g. when the Customer makes use of the Bank's technical support).

8. Communication Suite

8.1. Secure communication via the Communication Suite

The Communication Suite is an application that is automatically included within the functional scope of the Corporate Portal. The Customer and the Bank may communicate securely with each other via the Communication Suite.

Each User is provided with an individual Communication Suite through which the User may, acting on behalf of the Customer, receive notifications and documents from the Bank and send notifications and documents to the Bank. Notifications and documents are hereinafter collectively referred to as "Documents".

8.2. Communication by the Customer with the Bank

Within the scope of the power of attorney granted to the User by the Customer in the

Corporate Portal or otherwise, each User is authorised to submit legally binding declarations of intent to the Bank via the Communication Suite on behalf of the Customer and to electronically sign Documents made available by the Bank.

Orders submitted to the Bank via the Communication Suite are not processed automatically. Orders transmitted by a User to the Bank via the Communication Suite are processed in accordance with the legal and contractual provisions applicable to the respective type of order and within the proper operational procedures.

8.3. Communication by the Bank with the Customer

The Bank is entitled to upload Documents relating to the business relationship between the Customer and the Bank to the Communication Suite of one or more Users of its choice. This also includes content that may be relevant to one or more contractual relationships existing between the Bank and the Customer. The selection of the User or Users whose Communication Suite the Bank uses for uploading Documents shall be at the Bank's discretion. The Customer is responsible for ensuring internal forwarding and acknowledgment of such Documents and for implementing the organisational measures required within its organisation, including in order to comply with any review and objection obligations pursuant to No. 11 of the Bank's General Terms and Conditions.

The Bank fulfils any obligation to notify, transmit, inform or make Documents available by uploading them to the Communication Suite. The Bank is entitled to transmit Documents additionally or exclusively by post or by other means if this is necessary due to internal technical circumstances of the Bank or appears appropriate taking into account the Customer's interests, in particular in the event of technical disruptions or due to statutory or supervisory requirements.

The Customer agrees to the electronic transmission of invoices in accordance with section 14 of the German Value Added Tax Act (UStG).

Note for Customers subject to bookkeeping and record retention obligations: The Bank cannot guarantee that the Documents made available in the Communication Suite will be recognised by tax or fiscal authorities.

8.4. Integrity of data

The Bank ensures the immutability of the Documents uploaded to and stored in the Communication Suite.

8.5. Notification

The Bank informs the User of the uploading of new Documents to the Communication Suite via the communication channel agreed for this purpose (e.g. by email). The User is obliged to provide the Bank with the data required for such communication channel (e.g. an email address).

If the User fails to provide such data or if the data is no longer up to date, the Bank is entitled, but not obliged, to use another communication channel known to the Bank in the context of the business relationship with the Customer or the User for notification purposes.

If the User fails to comply with its obligation to provide the data required for notification, the Bank shall nevertheless remain entitled to upload Documents to the Communication Suite. In such case, it shall be the User's responsibility to regularly check the Communication Suite for new Documents.

8.6. Receipt

Documents shall be deemed to have been received by the Customer once they have been uploaded in retrievable and storable form to the Communication

Suite of at least one User, such User has been notified of the upload, and the User could have taken note of the Documents under ordinary circumstances.

If notification of the User by the Bank is not possible for reasons attributable to the Customer, in particular because the User has failed to comply with its obligation pursuant to Clause 8.5., Documents shall be deemed to have been received once they have been uploaded in retrievable and storable form to the User's Communication Suite and the User could have taken note of the Documents under ordinary circumstances.

In any event, a Document shall be deemed to have been received at the latest when a User has actually accessed the Document in the Communication Suite.

8.7. Obligation of regular check

It is the User's responsibility to regularly check the Communication Suite for newly uploaded Documents, in particular if a notification was not possible for reasons attributable to the User. Upon receipt of a notification, the User is obliged to take note of the Document without undue delay.

8.8. Provision and retention

The Bank makes the Documents uploaded by it to a User's Communication Suite available to the Customer in retrievable and storable form for a period of at least ten years from the date of upload. During this period, the Customer's access shall be possible only via the Communication Suite of the Users currently authorised.

If a User loses access to the Corporate Portal (e.g. due to withdrawal of power of attorney or deletion of the User status), the Customer shall no longer have access to the Documents stored in that User's Communication Suite.

Upon termination of the Agreement, the Customer's access to all Documents stored in the Communication Suites of its Users shall end.

It is the Customer's responsibility to download and store in its own systems all Documents required by it (e.g. for tax purposes) from the Corporate Portal prior to the deletion of access of the relevant User or prior to termination of the Corporate Portal agreement.

Statutory record retention obligations of the Bank shall remain unaffected.

9. Liability

9.1. General Exclusion of Liability

The liability of the Bank for claims of the Customer arising out of or in connection with the Agreement and the applications of the Corporate Portal shall be excluded and limited in accordance with the following provisions:

The Bank's liability for damage to property and purely financial loss resulting from simple negligence on the part of the Bank, its representatives and its vicarious agents shall be excluded.

For culpable breaches of material contractual obligations (wesentliche Vertragspflichten), the Bank shall be liable in accordance with statutory provisions, but such liability shall be limited in amount to damages that are typical and foreseeable under the agreement. Material contractual obligations are those obligations the fulfilment of which is a prerequisite for the proper performance of the agreement and on the observance of which the contractual partner may regularly rely.

Strict liability of the Bank in accordance with Section 536a(1), first alternative, of the German Civil Code (BGB), for defects already existing at the time the agreement was concluded, is hereby excluded.

In the following cases, the Bank shall always be liable in accordance with statutory provisions, irrespective of sentences 1 and 2 of this clause: in the event of grossly negligent or wilful misconduct of the Bank, its representatives or its vicarious agents; in the event of liability under the German Product Liability Act (Produkthaftungsgesetz); in the event of injury to life, body or health; or where the Bank, its representatives or its vicarious agents have fraudulently concealed a defect or have assumed a guarantee.

In the event that the Bank incurs any liability towards third parties who are not party hereto but with whom the contractual partner is in business contact in connection with the performance of this agreement, the contractual partner shall indemnify and hold the Bank harmless such that the Bank would not be liable towards the contractual partner under the above provisions.

9.2. Priority of special liability provisions

The liability provisions set out in these Terms and Conditions shall apply only insofar as mandatory statutory provisions or specific terms and conditions applicable to individual services or products – in particular transfer conditions, card conditions or comparable contractual provisions – do not contain deviating regulations.

In the event of any conflict, the statutory provisions and the respective other contractual conditions shall take precedence over the liability provisions of these Terms and Conditions.

10. Obligations of the Customer and the Users regarding Customer data

10.1. Obligations of the Customer and the Users regarding data storage

The User shall not store or use any files or data in the Corporate Portal, its applications or the Communication Suite that violate applicable law or the rights of third parties. Prior to storing or using data in the Corporate Portal, the User is obliged to check such data for viruses or other harmful elements by appropriate means (e.g. virus protection software).

10.2. Right of the Bank to delete customer data

The Bank is entitled at any time to delete Customer data if there is justified suspicion that such data violates the rights of third parties, these Terms and Conditions or applicable laws or regulations.

10.3. Obligation to perform data back-ups

The Customer shall be responsible for performing appropriate regular data back-ups in order to be able to use such data in the event of disruption or to retain such data in accordance with regulatory requirements.

11. Security measures of the Customer and the Users

The Customer shall ensure, prior to each access to the Corporate Portal, that standard market-compatible security measures (e.g. virus protection software and firewalls) are installed on the system used by the Customer or its Users and are regularly updated.

12. Availability

The Bank endeavours to ensure continuous availability of the Corporate Portal. However, temporary restrictions may occur due to updates, maintenance work or technical disruptions.

13. Updates

The Bank may, without being under any obligation to do so, update the Corporate Portal, its applications and the Communication Suite at any time and, in particular, adapt them due to changes in the legal framework, technological developments or to enhance IT security.

In doing so, the Bank shall reasonably take into account the Customer's legitimate interests and shall, where possible, inform the Customer of any necessary updates. In the event of a material impairment of the Customer's legitimate interests, the Customer shall be entitled to an extraordinary right of termination.

14. Right of amendment

The Bank is entitled to unilaterally amend, supplement, restrict or discontinue the functionalities, applications and the Communication Suite, provided that such changes

- are required in order to comply with statutory requirements or official or judicial orders or decisions;,
- are necessary to counter risks to the security of the Corporate Portal; or
- are reasonable for the Customer, taking into account the interests of the Bank.

Permissible changes shall include adaptations to the layout, navigation, user interface, structure and functional scope of the applications provided. The Bank may expand the Corporate Portal at any time by adding additional applications.

15. Termination

15.1. Termination of the Agreement

The Customer and the Bank may terminate the Agreement. The termination rights of the Customer and the Bank shall be governed by the Bank's General Terms and Conditions.

Termination of the Agreement shall automatically result in the termination of the applications included therein (see Clause 7).

15.2. Termination of application agreements

The Customer and the Bank may separately terminate an agreement relating to an application that has been concluded independently (see Clause 7.2). The termination rights of the Customer and the Bank shall be governed by the Bank's General Terms and Conditions. Where an application is subject to fees, termination shall only be effective at the end of a calendar month.

The Agreement shall remain in effect even if one or more application agreements are terminated.

15.3. Termination upon end of the business relationship

The Agreement and any agreements relating to applications shall automatically terminate as soon as no banking business relationship exists any longer between the Bank and the Customer other than the Agreement itself.

15.4. Deletion of the Customer's access to the Corporate Portal

The Bank is entitled to delete the Customer's access to the Corporate Portal without prior notice if the Customer or any User authorised for the respective application has not used the Corporate Portal for a period of at least twelve (12) months.

Non-use shall be deemed to exist if, within such period, no User of the Customer has logged into the Corporate Portal by means of its authentication elements.

16. Provisions governing contract conclusion on the Corporate Portal

The provisions of section 312i (1), sentence 1, nos. 1 to 3 of the German Civil Code (BGB) applicable to contracts concluded in electronic commerce shall not apply to contracts concluded via the Corporate Portal, its applications or the Communication Suite.

17. Governing law and jurisdiction

This Agreement shall be governed by the laws of the Federal Republic of Germany. All non-contractual rights and obligations arising out of or in connection with this agreement shall also be governed by the laws of the Federal Republic of Germany.

If the Customer has its registered office or place of residence in the EU, the UK, Switzerland, Norway or Iceland, the exclusive place of jurisdiction for all disputes arising out of or in connection with this Agreement shall be Munich, Germany.

If the Customer does not have its registered office or place of residence in the EU, the UK, Switzerland, Norway or Iceland, all disputes arising out of or in connection with this Agreement shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce (the "Rules") by an arbitrator appointed in accordance with the said Rules. The place of the arbitration proceedings shall be Munich. The language of the arbitration proceedings shall be English.