1. GENERAL PROVISIONS

1.1. These Special Terms and Conditions for Smart Data Basic ("ST&Cs") govern access to the Smart Data Portal, operated by Mastercard Europe SA, Chaussée de Tervuren 198A, 1410, Waterloo, Belgium ("Mastercard"), to the company credit cards ("Cards") issued by UniCredit Bank Austria AG ("the Bank") under a "Framework Agreement for Company Credit Cards", and the use of this service by the Company Program Administrator ("the CPA"), who serves as the contact and responsible person for the purposes of Smart Data for the company concluding the agreement for the use of Smart Data Basic ("the Company"). The natural person who acts as the CPA is only an authorised agent of the Company and not a contract partner of the Bank. These ST&Cs apply in addition to the "Terms and Conditions for Company Credit Cards of UniCredit Bank Austria AG" ("T&Cs"), as agreed between the Bank and the Company.

1.2. Use of Smart Data Basic requires at least an active Framework Agreement for Company Credit Cards, at least one valid credit card agreement for a company credit card ("Card Agreement") between the Bank and the Company, as well as the Company's application to use Smart Data Basic, which is accepted upon issuance of the access credentials for the Smart Data Portal.

2. SMART DATA PORTAL

2.1. The Smart Data Portal enables the CPA to view information about the Company's Bank Austria company credit cards, make enquiries (especially transaction enquiries), and view and download the transaction notice. The Smart Data Portal cannot be used to issue payment orders or legally binding declarations of intent, nor can the Card be used through the portal.

2.2. The Company shall be solely responsible, at its own expense, for procuring and maintaining the operating systems, software, hardware, and services that are required for its authorised users to access and use Smart Data.

2.3. Only the designated CPA shall be authorised to access Smart Data.

3. DEFINITION OF TERMS

3.1. User ID: The CPA shall receive a multidigit user ID as a personal security feature. The user ID cannot be changed. The user ID serves as the personal security feature for both the initial login and all subsequent logins to the Smart Data Portal by the CPA.

3.2. One-time password: The one-time password is used to verify the identity of the CPA during the initial login to the Smart Data Portal.

3.3. Password: The password is the combination of characters defined by the CPA during the initial login to the Smart Data Portal. The password is a personal security feature of the CPA, which, when used together with the user ID, serves to verify the CPA's identity for accessing the Smart Data Portal. The password can be changed by the CPA in the Smart Data Portal.

3.4. Security question/answer: The security question and answer were defined by the CPA when registering for the Smart Data Portal. The security question and answer are a personal security feature of the CPA, which, when used together with the user ID, serves to verify the CPA's identity for the purpose of resetting the password in the Smart Data Portal. The security question and answer can be changed by the CPA in the Smart Data Portal.

4. DUE DILIGENCE OBLIGATIONS AND RECOMMENDED SECURITY MEASURES

The Company must ensure that only the access-authorised user it has designated (CPA) logs in to the Smart Data Portal and that the personal security features are used to access the Smart Data tool only by the person to whom they were issued. All actions taken by authorised employees in connection with the Smart Data Portal shall be directly attributable to the Company. The Company shall be obligated to comply with the due diligence obligations set out below.

4.1. Secrecy and blocking obligation

(1) The Company shall be obligated to ensure that the CPA takes all reasonable precautions to maintain the secrecy of the personal security features (password, one-time password, user ID, and security question/answer). Insofar as would be considered reasonable, neither the Company nor the CPA shall share this information with unauthorised third parties, including employees of the Bank, or act in a similar way based on their own decision-making.

(2) The Company shall be obligated to exercise the utmost care in storing and using the personal security features so as to prevent unauthorised access to the Smart Data Portal. They may not be written down or stored (e.g. in a note-taking app) on the device used to access the Smart Data Portal or on the device to which the personal security features are delivered.

(3) If personal security features are lost or stolen or if the Company becomes aware of any misuse or other

unauthorised use of the Smart Data Portal, it must immediately arrange for access to the Smart Data Portal to be blocked (tel.: +43 5 05 05-25). When reporting by telephone, the caller must verify his/her identity and authorisation to report the information as an authorised agent of the Company by providing personal data.

(4) The Company must ensure that the CPA complies with these due diligence obligations.

4.2. Recommended security measures for use of the Smart Data Portal

(1) It is recommended that the chosen password be changed regularly, at least every two months, on the user's own initiative.

(2) It is recommended to immediately change the password or arrange for access to the Smart Data Portal to be blocked if there is reason to believe that unauthorised third parties have gained knowledge of the personal security features or if other circumstances exist that could enable misuse by an unauthorised third party.

5. BLOCK

5.1. Access to Smart Data shall be blocked if the password is entered incorrectly six consecutive times during a single access attempt. Access shall also be blocked if the CPA does not log in to Smart Data at least once within a period of 90 days.

5.2. The Company can request that access to the Smart Data tool be blocked at any time.

5.3. The Bank shall be entitled to block Smart Data if there are objective security-related reasons that justify such action or there is a suspicion of unauthorised or fraudulent use. The Bank shall lift a block as soon as the reasons for the block no longer apply or the CPA requests that the block be lifted.

6. TERM AND TERMINATION OF THE AGREEMENT

6.1. The agreement on participation in Smart Data shall be concluded for an indefinite period of time. However, it shall end automatically immediately if there is no longer an active Framework Agreement for Company Credit Cards between the Company and the Bank.

6.2. The Bank and the Company can terminate the agreement on participation in Smart Data Basic at any time subject to a reasonable period of notice. Any fees paid in advance shall not be refunded.

6.3. Both the Company and the Bank shall be entitled to terminate the agreement on participation in Smart Data Basic at any time with immediate effect for important reasons.

6.4. Termination of the agreement on participation in Smart Data Basic shall not affect the existing Framework Agreement for Company Credit Cards or any card agreements concluded under it, unless the Company and/or the Bank also terminate the Framework Agreement at the same time.

7. AMENDMENTS TO THE TERMS AND CONDITIONS

7.1. Amendments to these ST&Cs must be agreed.

7.1.1. This can also occur by way of the following procedure: Amendments to these ST&Cs are proposed to the Company by the Bank in a timely manner so that the amendment notice is received two months before the proposed date of the entry into force at the latest. If the Bank has received no objections from the Company by the proposed date of the entry into force, this shall represent tacit acceptance on the part of the Company. The Bank shall inform the Company of this fact in the amendment proposal. The Company shall be informed of the amendment proposal. The Company shall be entitled to terminate the agreement on participation in Smart Data immediately at no charge before the amendments go into effect. The Bank shall include notice of this fact in the amendment proposal.

7.1.2. The notice defined in item 7.1.1. shall generally be sent by regular mail to the address most recently provided by the Company. The Bank shall deviate from this general procedure and submit this notice in electronic form via the online banking mailbox if the Company has concluded an agreement for the use of online banking with the Bank. This electronic notice shall be made in such a way that the Bank can no longer make unilateral changes to the amendment proposal and the Company can save and print out the notice.

8. CHANGES TO OBLIGATIONS AND SERVICES

8.1. The Bank may change, at its reasonable discretion, the material contractual obligations of the Bank or the Company, taking into account all relevant circumstances (particularly changes in the legal framework, changes on the money or capital market, changes in refinancing costs, changes in staff and non-staff expenses, etc.). Within these limitations, the Bank shall also be entitled to introduce new services that are subject to fees as well as new fees for services that have already been agreed.

8.2. Beyond the provisions defined in item 8.1, the Bank can propose changes to the mutual services and fees (changes specified in item 8.1 and changes above and beyond this) via the procedure defined in item 7.1.

9. CHOICE OF LAW AND COURT OF JURISDICTION

9.1. The place of performance is Vienna.

9.2. The contractual legal relationship shall be subject to Austrian law, under exclusion of the UN Convention on Contracts for the International Sale of Goods.

10. VALIDITY OF THE CARD

10.1. The validity of the Card shall end at the end of the month specified on the Card in the year specified on the Card. The use of an invalid card is not permitted, but shall not affect the Company's obligation to pay for goods and services purchased with such a card.

10.2. The Bank shall issue a new card for a further validity period in a timely manner before the expiration of the Card.

10.3. The Company may only file suits against the Bank at the competent court at the registered office of the Bank's headquarters. This shall also be the court of jurisdiction for suits filed by the Bank against the Company. However, the Bank shall be entitled to assert its rights in any other competent court regardless of location.