

		REQUEST for using the Digital Documents Exchange (DDE) Platform for Legal Entities (LEs)			
Please select the desired action:					
First time registration	<input type="checkbox"/>				
Changing existing registration	<input type="checkbox"/>				
<i>Please read the Instructions for completing the form (Section VI), which can be found on the last page. The fields marked with an asterisk (*) are mandatory. Please write legibly in CAPITAL LETTERS.</i>					
I. Client data		Client number*			
Name*					
BULSTAT/ UIC*					
II. Information about Legal Representative(s)/Proxy(ies):					
1. First name, middle name, family name*		Add	<input type="checkbox"/>	Remove	<input type="checkbox"/>
Personal ID Number/Personal foreigner's number/date of birth (for foreigners)*					
Contact details to obtain a username, password and access code for the DDE platform <i>This data will be used for all LEs to which you are subscribed. For an existing user subscribed to another LE, the e-mail and phone number specified in the previous request will be used. In case you want a new e-mail and/or phone number to be used, please specify them.</i>					
Registration e-mail*				Mobile phone number*	
Information for receiving notifications from DDE <i>"E-mail for notifications" can only be used if the user is subscribed to more than one LE. This e-mail will only be used to receive notifications related to the exchange of documents only for the specific LE that initiated this request.</i>					
Same as above <input type="checkbox"/>					
E-mail for notifications					
2. First name, middle name, family name*		Add	<input type="checkbox"/>	Remove	<input type="checkbox"/>
Personal ID Number/Personal foreigner's number/date of birth (for foreigners)*					
Contact details to obtain a username, password and access code for the DDE platform <i>This data will be used for all LEs to which you are subscribed. For an existing user subscribed to another LE, the e-mail and phone number specified in the previous request will be used. In case you want a new e-mail and/or phone number to be used, please specify them.</i>					
Registration e-mail*				Mobile phone number*	
Information for receiving notifications from DDE <i>"E-mail for notifications" can only be used if the user is subscribed to more than one LE. This e-mail will only be used to receive notifications related to the exchange of documents only for the specific LE that initiated this request.</i>					
Same as above <input type="checkbox"/>					
E-mail for notifications					
3. First name, middle name, family name*		Add	<input type="checkbox"/>	Remove	<input type="checkbox"/>
Personal ID Number/Personal foreigner's number/date of birth (for foreigners)*					
Contact details to obtain a username, password and access code for the DDE platform <i>This data will be used for all LEs to which you are subscribed. For an existing user subscribed to another LE, the e-mail and phone number specified in the previous request will be used. In case you want a new e-mail and/or phone number to be used, please specify them.</i>					
Registration e-mail*				Mobile phone number*	
Information for receiving notifications from DDE <i>"E-mail for notifications" can only be used if the user is subscribed to more than one LE. This e-mail will only be used to receive notifications related to the exchange of documents only for the specific LE that initiated this request.</i>					



Same as above <input type="checkbox"/>							
E-mail for notifications							
4. First name, middle name, family name*				Add	<input type="checkbox"/>	Remove	<input type="checkbox"/>
Personal ID Number/Personal foreigner's number/date of birth (for foreigners)*							
Contact details to obtain a username, password and access code for the DDE platform <i>This data will be used for all LEs to which you are subscribed. For an existing user subscribed to another LE, the e-mail and phone number specified in the previous request will be used. In case you want a new e-mail and/or phone number to be used, please specify them.</i>							
Registration e-mail*			Mobile phone number*				
Information for receiving notifications from DDE <i>"E-mail for notifications" can only be used if the user is subscribed to more than one LE. This e-mail will only be used to receive notifications related to the exchange of documents only for the specific LE that initiated this request.</i>							
Same as above <input type="checkbox"/>							
E-mail for notifications							

III. Conditions, statements, obligations and responsibilities

- The Bank will provide the Client and each User with the following services:
- Access to the Digital Document Exchange platform (hereinafter referred to as **DDE platform/the Platform**), representing a secure, closed channel for maintaining communication between the Bank and the Client, as well as for sharing documents.
- When access is granted to the Client and each User, the Platform will provide a technical possibility for digital signing with a qualified electronic signature (QES) of agreements and documents. It is not allowed to sign documents through the Platform, for which a qualified written form is required by the law or when holding the document or a copy thereof has legal significance (e.g. promissory note/bills of exchange), including also documents containing payment instructions. Except the legal representative(s), each User having active access should also have an additional notary-certified power of attorney deposited with the Bank, by which they have been granted the right to conclude/sign a relevant type of agreement and/or document, the User's authority to sign having been checked by the Bank before sending the agreement/document to the User for signing it.
- Using the DDE platform, the Bank will provide a suitable framework for concluding agreements or signing documents electronically with the Bank's Clients. As part of the framework, in collaboration with Namirial S.p.A, [Italian company based in Senigallia (Ancona), postal code 60019, Via Caduti sul Lavoro 4, Italy, entered in the Commercial Register of Ancona, having tax number/VAT number 02046570426/No 02046570426 (Provider of qualified authentication services within the meaning of the eIDAS Regulation), hereinafter: **Namirial**], under Act LIII of 2017 on Preventing and Combating Money Laundering and Terrorist Financing (hereinafter: AML law) for identified clients, the Bank will provide an opportunity in the Platform, Namirial to issue a one-time Qualified Electronic Signature Certificate for residents of the Republic of Bulgaria (Bulgarian citizens and foreigners who are permitted to reside in the Republic of Bulgaria) and who certify their right of residence using a residence permit issued by the Ministry of Interior and/or a certificate of residence of EU citizens issued by the Ministry of Interior) when signing agreements/documents by the Client and any User having access in accordance with the applicable General Terms and Conditions of Namirial (the services described in this paragraph hereinafter referred to as: the Service).
- By signing this request, the Client and each User agree to sign and/ or exchange documents signed with a Qualified Electronic Signature through the Platform. The Client and/or each User undertakes to ensure the signing of the document by the parties thereto (with the exception of the Bank) with qualified electronic signatures, of which, should the relevant Parties (other than the Bank) are legal entities, the holders are the relevant legal entities, and authors - the natural persons indicated as representatives of such Parties in the electronic document, and/or should the relevant Parties (other than the Bank) are legal entities, holders and authors are the natural persons indicated as representatives of such Parties in the electronic document and their qualified electronic signatures contain as a requisite their unique identification number (Personal ID Number, Personal number of a foreigner or other number applicable to foreign citizens).
- The Client and each User will accept that the provision of an e-mail address and a telephone number is an essential element for the use of the Service. The Client and the User will jointly be entitled to amend the above-mentioned information by means of a new Request for use of a Digital documents exchange platform (DDE) for LEs (hereinafter: a Request/ the Request). The Bank will not be responsible for damages resulting from failure to notify it of the Client/User information amendment.
- By sending a one-time password for initial registration on the Platform, the Bank confirms that it provides access of the Client and/or the relevant User to the Platform and undertakes to ensure the use of the Service in accordance with the access granted.
- The Client and each User declares that they will use the Service based on the Request submitted and for the benefit of the Client and in accordance with their duly established representative authority. The User may access the Service for several clients at the same time and at different times. The User accepts that the accesses related to the DDE Platform will be specified by each Client. The Bank considers the last Request for access to the Platform submitted by the relevant Client to be valid and based thereon it will manage (correct/change) access/data in the User's Platform. The Client hereby confirms that the Bank is not responsible for damages resulting from a change in access/data in the User's Platform, of which it is not duly and promptly notified.

9. As part of the Service, Namirial will provide a one-time Qualified Electronic Signature Certificate. The User confirms that they have been notified and agree that should the Bank obtains rights from the Client (role) to access the Service, it will transfer the registration and identification data of the User to Namirial. The User expressly consents to the transfer of such data by signing this document/this Request. The Client and each User will enter into an agreement with Namirial as regards the use of the electronic signature service as part of the electronic signature process.

10. Within the meaning of art. 62 of the Credit Institutions Act, by signing this Request the Client declares their written consent to the disclosure to the above-mentioned Users of facts and circumstances representing banking and/or trade secrets and releases UniCredit Bulbank AD from any liability in disclosure of bank information which may constitute the Client's banking and/or trade secret - in connection with the use of the Platform by the Users specified by the Client.

11. The Client and each User specified herein will declare that they are aware of and undertake to fully comply with the Security Requirements specified specified in Appendix No 1 hereinbelow.

12. The Bank will be entitled to restrict a Client/User's access to the Service at any time in the event of non-compliance, suspicion of non-compliance with the rules for using the service, security recommendations or a risk identified by it relating to the use of the Service by a Client/ User.

13. The Client and each User will be obliged to keep secret all their electronic identification means on the Platform by creating conditions excluding any possibility of unauthorised access by third parties. The risk and responsibility for failure to protect the secrecy of the electronic identification means will remain for the account of the Client. The Client will be responsible for their own account and will be bound by all actions and consequences thereof performed on their behalf after gaining access to the Platform by using the electronic identification means.

14. In the event of reasonable suspicion that the electronic identification means of a Client and each User have become known to/ acquired by other unauthorised persons, and/or the relevant mobile devices and computers have been lost, stolen, and/or there is a suspicion of information leakage, the Client and each User will be obliged.

15. The Bank will consider the access initiated by the Client and each User logged into the Platform interface by using the identification means (mobile phone, username, password) and authenticated with the one-time password sent to the Client's device and/ or each User as initiated by the person, specified in this Request, and will not verify the authorisation of the Client/User of their identification means and password (mobile phone) and terms of use. The Bank will not be responsible for damages caused to the User or the Client when accessing the Service, initiated by using his identification means and authenticated with the relevant password, but originating from an unauthorised person.

16. Even after due care, when using a telephone device or the Internet in connection with the work on the Platform, there may be cases in which the exchanged messages become known to unauthorised third parties. In view of this, the Client and each User acknowledges that they assume risks by using and benefiting from the Service, and that they have decided to use the Service after assessing such risk. In this regard, the Bank, in accordance with the confirmation and consent within the meaning of point 8 (eight) hereinabove, will not be responsible if information considered as bank secret transmitted during electronic communication through the Platform becomes known to unauthorised third parties.

17. The Bank will be liable to the Client for losses suffered by them, insofar as they are a direct and immediate consequence of non-fulfilment of the Bank's obligations to provide the Service established by this document/this Request, committed intentionally or through gross negligence.

18. The Bank will not be responsible in case of non-fulfilment of its obligations to provide the Service due to lack of contractual relations of the Client and each User with a mobile operator, technical problems with the mobile operator or the device of the Client and each User (e.g. lack of coverage, roaming coverage, disconnected phone, etc.) and any reasons due to technical/ communication failures and/or other events beyond the will and control of the Bank, including but not limited to technical malfunction, inappropriate security settings and inappropriate security level of the device, from which the Service is accessed.

19. The Bank will not be responsible in the event that the Client and each User does not have the necessary licenses to use the other software products required to work with the Platform. This also includes the cases where the Client and every User uses unlicensed software, as this creates a prerequisite for infecting their computer equipment with malicious code.

20. The Bank will be released from responsibility for fulfilling the obligation to send a one-time password and access codes via SMS related to the operation of the Platform based on the information it has and that it has initiated such SMS without being obliged to prove their receipt by the Client/ User. The Bank does not check whether the provided telephone number is owned by the client/User.

21. The Client and the User will be fully financially liable in case of illegal use of a mobile phone number entered in the Service in the following cases: providing a false mobile phone number; failure to notify/untimely notification to the Bank of a change of mobile phone number or theft of a SIM card to which the relevant mobile phone number entered in the Service is directed.

22. The Bank is not obliged to notify the Client and the User of changes representing an expansion of the scope of the Service provided, of changes made related to the technical support and development of the Platform with the aim of improving the Platform's operability, as well as of such changes resulting from changes in regulations/ current legislation.

23. The Bank reserves the right to change the means of identification, authorisation and their combinations by notifying its Clients in a period not less than two months before the date on which the changes are proposed to enter into force through the Bank's official page or another appropriate way, including if it is necessary for the Clients to appear at the Bank and receive the new means of identification and authorization. Where applicable, together with the notification under the preceding sentence, the Bank will inform the Client that it considers the latter to have accepted the changes, unless it notifies the Bank that it does not accept such changes before the date on which they come into force. In these cases, the Bank will notify the Client that the latter is entitled to terminate access to the Platform and use of the Service prior to the date on which the changes are proposed to take effect.

24. Upon termination of business relationships with the Client, including but not limited to closing all Client's accounts, access to the DDE Platform will also be terminated, for which the Client gives his express, unconditional and irrevocable consent by signing this Request. The Bank will notify the Client of the termination of access to the Platform through an automatically generated e-mail sent by the Platform.

25. By signing this Request, the Client and each User give explicit and unconditional consent to make searches/ collect information with government bodies, institutions, establishments and registers (Regix, Ministry of Interior, etc.) for the purposes of signing up the DDE Platform and use of the Service by Namirial. By signing the Request, the Client and each User declare that they agree to the carrying out of searches and the processing of their personal data, including data that could constitute a trade secret, to obtain preliminary information for the purposes of providing access/ signing up on/ in the Platform.

Appendix No 1

Security requirements for using the DDE platform by the Client and Users

*For the safe use of the means of communication used by the Client/User when using the Platform [in particular, but not only: smartphone, computer (desktop/ laptop), tablet, including software and hardware elements and e-mail (hereinafter: **Device**)] to make valid electronic statements of will binding on the Client, including signing an agreement and using the Platform, as well as to preserve the Client's/User's personal data and the Client's bank secrets, the proper maintenance and security of these Devices will be essential and the continuous fulfillment of the following security requirements will be necessary, for which the Client and the User will be jointly responsible:*

- *the device is accessible only and exclusively after successful identification of the Client/User on the device, and the data used for identification is changed regularly and may not be easily guessed (PIN code — for smartphones/for tablets, password);*
- *the elements of the Device (operating system, firmware, browser, other applications) are regularly updated in accordance with the manufacturer's recommendations and are professionally and securely set up;*
- *the Device's network connections are set up securely using appropriate wireless network security procedures (e.g. encryption and authentication), restricting access to network devices;*
- *the display of the Device is visible only to the Client/User during the process;*
- *saving the username and password in the browser is not recommended;*
- *it is recommended to use a password that is at least 9 characters long, contains lower- and upper-case letters, numbers, special characters, does not contain meaningful words from the dictionary, the usage of a special password is recommended, and it is recommended that the Client/User avoids re-using passwords, used for other services, it is generally recommended to use a secure password store.*

In addition to the above, in respect of smartphones/tablets:

- *security mechanisms, the authorisation system and other subsystems of the operating system are not modified on the device (root - Android, jailbreak - iOS);*
- *SMS viewing is not allowed on lock screen;*
- *The PIN code does not contain data that can be easily known, e.g. date of birth, recurring characters, e.g. 111111.*

In respect of desktop/laptop, in addition to the above:

- *has a legitimate, up-to-date protection against malicious code (virus protection, anti-malware) – virus scanning is performed regularly and its scope extends to downloaded files, data carriers connected to the device, with modern security solutions (e.g. firewall).*

In addition, the Client/User guarantees that when using the Platform for the exchange of digital documents electronically, the communication tools used to make an electronic statement accessible only to the Client/User, and access by third parties is impossible.

The Bank reserves the right - but is not obliged - to limit the types of messages delivered without special notice, to pause or terminate the sending of messages, to suspend or limit the operation of the access provided by the Bank to the Platform on devices operating with an operating a system modified by the manufacturer or the Client/User in such a way that the Client/ User's access to the operating system or its subsystems is not limited (including, but not limited to: "jailbreak", "unlock", "root" and similar modifications) or the modification of the operating system may carry other data security risks - an outdated and vulnerable version of the browser or operating system is used. Browser-based systems and applications may contain software code to modify the operating system and/ or check the version of the browser and/or operating system, and information about the modified operating system may be forwarded by the application to the Bank.

IV. Information on personal data processed by UniCredit Bulbank AD, according to EU Regulation 2016/679 (General Data Protection Regulation):

UniCredit Bulbank AD, UIC 831919536, having its seat and registered office at: Sofia, 7 Sveta Nedelya Square, bearing a license to perform banking activities issued by the Bulgarian National Bank by Order No RD22-2249/16.11.2009, is a controller.

To provide this service - issuing of a one-time electronic signature for the purpose of digital signing of documents in connection with banking services/products provided, UniCredit Bulbank AD, in cooperation with Namirial S.p.A., will process your personal data on a valid legal basis - subscribing to the service.

For the purposes specified hereinabove, the subject of processing will be personal data that will include, but will be not limited to: credentials (names, unique personal identifier or date of birth, identity document), contact details (such as e-mail, phone number, user name, password for use).

The bank will process your personal data **for the purposes** of performing banking activities and managing relationships with clients, before and/or during validity of concluded banking agreements. Should you apply for a credit product, the Bank will have to process your personal data for the purposes of assessing creditworthiness. Also, if you have given your consent, your personal data will be processed for direct marketing purposes by analysing information about your preferences and purchasing habits and promoting the products and services offered by the Bank. Your personal data may be processed to investigate your satisfaction and improve client service, unless you object to such processing. In order to control the activities of external services providers, for security and protection reasons, as well as for the prevention of fraud, information that constitutes personal data will be also processed. UniCredit Bulbank AD is under a statutory obligation to process your personal data for the purposes of preventing money laundering and financing of terrorism. According to the Measures against Money Laundering Act, to identify the person carrying out the operation, i.e. to process personal data from the identity document, including when the person is not its client. This processing will also include fulfillment of the statutory obligation to check and take a copy of the identity document, the operations being performed using legally permitted technical means. The data will be processed and stored for the period and purpose established in the Personal Data Protection Act. The Bank will be also obliged to process your personal data when you are a representative of a legal entity – a client of the Bank. Your personal data will only be processed for the purposes for which it was collected.

The Bank will process personal data should at least **one of the grounds** for processing is present, namely: consent provided by you; when you wish to conclude or if you have already concluded an agreement with the Bank; to comply with a statutory obligation; for the purposes of the legitimate interests of UniCredit Bulbank AD. If you do not provide your personal data, the Bank will not be able to provide you with the Service you wish to receive.

Where a statute so provides or if it stipulated in your agreement, UniCredit Bulbank AD may disclose personal data to various **categories of recipients**:

- public authorities, institutions and establishments, auditors supervising the Bank's activities or compliance with a law applicable to the Bank or the data subjects. Such can be, for example, the Bulgarian National Bank, the Financial Supervision Commission, the Commission for Personal Data Protection, the National Revenue Agency, the State Agency for National Security, the Ministry of Interior, the court, the prosecutor's office, etc.;
- of processors operating under supervision of the Bank (including persons providing assistance in connection with the service and collection of claims of the administrator);
- to persons related to the Bank, including UniCredit Group companies, where there are justified legitimate interests of UniCredit Bulbank AD. In various processes related to direct marketing, connectivity assessment, maintenance and management of information systems (such as the current platform for digital signing of documents), regulatory reporting, sale of products and services, etc., UniCredit Bulbank AD and the Bank's subsidiaries in Bulgaria (UniCredit Consumer Financing, UniCredit Leasing, UniCredit Insurance Broker, UniCredit Fleet Management) may act as joint administrators and jointly determine the purposes and means of personal data processing;
- to third parties where there is a valid legal basis for the disclosure;
- where transferring (assigning) the receivables to third parties, subject to compliance with the requirements of the current legislation in the country.

As a rule, UniCredit Bulbank AD will **not transfer personal data to third countries** or international organisations. If this is still necessary, the provisions of the General Data Protection Regulation will be observed. Such a transfer will take place, for example, where it is necessary for the conclusion and execution of an agreement between you and the Bank. Such are the cases where you wish to make a money transfer abroad. You can use the Bank's telephone numbers or contact form (available on our site) to obtain information about the applicable guarantees for protection of your personal data and terms and conditions for data transfer.

UniCredit Bulbank AD will process your personal data within **the time periods** established by the regulatory supervisory authorities and the current legislation in the country. Personal data for which there is no express statutory/supervisory storage obligation will be deleted after achieving the purposes for which the personal data was collected and processed.

For certain categories of credit products (for example, those having a pre-approved limit), you may be subject to automated decision-making, including profiling, when assessing your creditworthiness. This type of decision-making will be necessary to conclude the agreement. For this purpose, various checks will be carried out in the Bank's databases and in the country's official registers, which result into the decision based on pre-set criteria. You may receive an offer for this type of product if you have previously given your consent to the processing of your personal data for direct marketing purposes. The decision whether to accept the offer will be entirely yours.

We inform you that according to the General Data Protection Regulation, you are entitled to request access to correct, delete or restrict the processing of your personal data, as well as the right to data portability. You are entitled to object to processing based on legitimate interest. If consent has been given for a specific purpose, you may withdraw it at any time without affecting the lawfulness of the processing before its withdrawal.

You can get more information about the personal data that UniCredit Bulbank AD processes on the Bank's website, www.unicreditbulbank.bg, section "Personal data protection", as well as at a bank branch // center convenient for you.

You can contact the Personal Data Protection Officer of UniCredit Bulbank using the following contact details: **DPO@UniCreditGroup.BG**, 7 Sveta Nedelya Square, Sofia 1000, Bulgaria.

If you believe that your rights as regards processing of personal data have been violated, you may file a complaint with the Commission for Personal Data Protection.

I/We declare the accuracy of the data specified by me/us in the Request and that I am/we are familiar with and accept the conditions specified herein for provision of the service "use of Digital documents exchange platform (DDE)" service:

Signature of the Client's representative (legal entity):

Full name: (.....)

Signature of the Client's representative (legal entity):

Full name: (.....)

Signature of the Client's representative (legal entity):

Full name: (.....)

Signature of the Client's representative (legal entity):

Full name: (.....)

Signature of User 1 of the Client (natural person):

Full name: (.....)

Signature of User 2 of the Client (natural person):

Full name: (.....)

Signature of User 3 of the Client (natural person):

Full name: (.....)

Signature of User 4 of the Client (natural person):

Full name: (.....)

VI. Instructions for completing the form

Dear clients, correct completion of the Request will help you get registration as quickly and accurately as possible. Thank you!

1. Select the right type of action you want to perform:

1.1. Initial registration – will be selected upon initial signing up on the DDE Platform;

1.2. Amendment of the existing registration - where adding or removing/disabling the access of the Client's Users to the DDE Platform; for any amendment, with the exception of removing/deactivating user's access, a signature will be required by both the legal representative(s) of the Client and the respective User(s).

2. In Section I. "Client Data", complete the data of the legal entity that will subscribe to use the DDE Platform.

3. In section II. "Data for Legal Representative(s)/Power(s) of Attorney": the data of the persons to be registered as Client's Users of the DDE Platform having specifically assigned access will be specified. The Client, acting through their legal representative(s), will express their will a specific natural person to access the DDE Platform as a User by signing this Request. The username for the DDE Platform will be provided/sent by the Bank and will be received by the Client's User at the User's registration e-mail/e-mail specified in this Request. The initial one-time password for accessing the DDE Platform will be sent by the Bank and received by the User via SMS to the mobile phone number specified in this Request. This one-time password will have the validity specified in the SMS sent and needs to be changed upon initial login to the DDE Platform. The e-mail address (e-mail for sending notifications) of the User specified in this Request will be used for subsequent sending of notifications from the Bank to the User, related to actions and/or the need to perform such actions in the DDE Platform. All signatures expressly designated as "Client's User Signature" will be signed solely by the specific Client's User.

4. If it is necessary to add more Users, the Client, acting through their legal representative(s), will complete new Request for use of digital document exchange (DDE) Platform. If it is necessary to revoke the access rights to the DDE Platform of an existing User(s) (removal of User(s)), the Client, acting through their legal representative(s), will complete new Request for use of digital document exchange (DDE) Platform.

5. Section III. "Conditions, statements, obligations and responsibilities" describes the obligations and responsibilities of the Client, Users and the Bank.

5.1. In Appendix No 1 in the same section III, the security requirements for using the DDE Platform are described.

6. In section IV. is provided "Information on personal data processed by UniCredit Bulbank AD, according to EU Regulation 2016/679 (General Data Protection Regulation)".

The following fields are mandatory and should be completed by a bank employee:

Date and time of receiving the Request:				Bank client OPU	
Details of the employee who accepted the request:					
	Name, family name, position	Ref.	structural unit number	Structural unit name	Signature: