Приложение № 1
Изискванията за сигурност при използване на DDE платформата от Клиента и Потребителя

За безопасната употреба на използваните от Клиента / Потребителя средства за комуникация при използване на Платформата [по-специално, но не само: смартфон, компютър (настолен/лаптоп), таблет, включително софтуерни и хардуерни елементи и електронна поща (наричани по-нататък: Устройство)] за отправяне на валидно обвързващи Клиента електронни волеизявления, включително подписване на договор и използване на Платформата, както и за да се запазят личните данни на Клиента /Потребителя и банковите тайни на Клиента, правилната поддръжка и сигурност на тези Устройства е от съществено значение и е необходимо непрекъснатото изпълнение на следните изисквания за сигурност, за които Клиентът и Потребителят носят пълната отговорност при условията на солидарност:

- *устройството е достъпно само и изключително след успешна идентификация на Клиента/Потребителя на устройството, като данните, използвани за идентификация, се променят редовно и не могат лесно да бъдат отгатнати (ПИН код — за смартфони / таблети, парола)*
- *елементите на Устройството (операционна система, фърмуер, браузър, други приложения) се актуализират редовно в съответствие с препоръките на производителя и са професионално и сигурно настроени*
- *мрежовите връзки на Устройството са настроени сигурно [като се използват подходящи процедури за защита на безжичната мрежа (напр. криптиране и удостоверяване), ограничаване на достъпа до мрежови устройства]*
- *дисплеят на Устройството е видим само за Клиента /Потребителя по време на процеса*
- *записването на потребителското име и паролата в браузъра не се препоръчва*
- *препоръчително е да използвате парола, която е дълга поне 9 символа, съдържаща малки и главни букви, цифри, специални знаци, не съдържаща смислени думи от речника, препоръчва се използването на специална парола, препоръчително е Клиентът /Потребителят да избягва повторната употреба на пароли, използвани за други услуги, обикновено се препоръчва използването на защитено хранилище за пароли.*

В допълнение към горното, по отношение на смартфони/таблети:

- *механизмите за защита, системата за оторизация и други подсистеми на операционната система не са модифицирани на устройството (root — Android, jailbreak — iOS)*
- *прегледът на SMS не е разрешен на заключен екран*
- *ПИН кодът не съдържа данни, които лесно могат да бъдат познати, напр. дата на раждане, повтарящи се знаци, напр. 111111.*

По отношение на настолен компютър / лаптоп, в допълнение към горното:

- *има легитимна, актуална защита от злонамерен код (защита от вируси, анти-малуер) – проверката за вируси се изпълнява редовно и нейният обхват се простира до изтеглени файлове, носители на данни, свързани към устройството, с модерни решения за защита (напр. защитна стена).*

Освен това Клиентът / Потребителят гарантира, че когато използва Платформата за обмен на документи по електронен път, комуникационните инструменти, използвани за правене на електронна правна декларация, са достъпни само за Клиента/Потребителя, а достъпът на трети страни е изключен.

Банката си запазва правото – но не е длъжна – да ограничи видовете съобщения, доставяни без специално предупреждение, да постави на пауза или да прекрати изпращането на съобщения, да спре или да ограничи работата на предоставения от Банката достъп до Платформата на устройства, работещи с операционна система, модифицирана от производителя или Клиента /Потребителя по начин, при който достъпът на Клиента / Потребителя до операционната система или нейните подсистеми не е ограничен (включително, но не само до: „jailbreak“, „unlock“, „root“ и подобни модификации) или модификацията на операционната система може да носи други рискове за сигурността на данните — използва се остаряла и уязвима версия на браузър или операционна система. Системите и приложенията, работещи в браузъра, могат да съдържат софтуерен код за промяна на операционната система и/или проверка на версията на браузъра и/или операционната система, като информацията за модифицираната операционна система може да бъде препратена от приложението към Банката.