Privacy and Cookies Policy

Privacy policy

Our Privacy Policy is set out in our General Terms and Conditions, in particular in the provisions of dealing with data protection, processing and use, and with banking secrecy.

When you use the Private eBanking service, we may automatically collect and store certain information in server logs, including without limitation Internet protocol (IP) addresses, Internet service provider (ISP), clickstream data, browser type and language, viewed and exit pages and dates or time stamps which we use for internal reporting and audit purposes.

Your use of the Private eBanking service with a portable device (smartphone, tablet or similar) will operate via an application (App) installed on your portable device, for which we may collect the following additional information about you:

(i) *Submitted information*
Information that you provide by filling in forms, either electronically or manually by hand. This includes information provided at the time of registering to use the App.

(ii) *Additional information*
If you contact us, we may keep a record of that correspondence.

(iii) *Device information*
We may collect information about the portable device or computer you may use to download or stream a copy of the App onto your portable device, including, where available, the portable device's unique identifiers, operating system, browser type and mobile network information as well as the portable device's telephone number for system administration. We may associate such Device information with Submitted information and will treat the combined information as personal data for as long as it is combined.

(iv) *Location information*
Your use of the Private eBanking service with a portable device may allow us to identify your location, and we may collect and process information about that location. Private eBanking services when accessed through a portable device may require your personal data for some of its features to work. If you wish the particular feature, you will be asked to consent to your data being used for this purpose. You can withdraw your consent at any time via the App's preference.

Cookies policy

This Cookies Policy explains our limited use of cookies and of information which is collected by the cookies in the provision of the Private eBanking service. By using the Private eBanking service you consent to the use of the cookies set out in this Cookies Policy. We only use cookies and the information obtained through them to deliver service functionality and enhance the security of the Private eBanking service. If you cease to use the Private eBanking service we will not read the cookies or use the information obtained thorough them. However, the cookies cannot be disabled when you use the Private eBanking service.

1. What are cookies and how are they used?

Cookies are text files containing small amounts of information which are downloaded to your computer or portable device when you visit a website or other Internet -enabled service. Upon your subsequent visits to the originating web domain, cookies are sent back to that domain, which thus has access to the information stored in the cookies. This notably allows a website or other Internet -enabled service to recognise the computer or portable device from which you access the site or service and remember the choices you make (such as your user name, language or region you are in).

The cookies we use are stored in the application of the Secure USB Device where you access the Private eBanking service through a computer; where you access the Private eBanking service through a portable device (smartphone, tablet or similar), the cookies are stored in the App you download to such device.

2. Why do we use cookies?

Identifying your computer or portable device and remembering your preferences enables us to provide you with personal features and allows you to navigate between pages efficiently, generally improving your user experience.

Identifying when you log in and off the Private eBanking service also enable us to implement security measures making your use of the Private eBanking service more secure.

3. What types of cookies do we use? *Session Cookies vs. Persistent Cookies*

Session cookies are deleted automatically when you close your browser and remove your Secure USB Device.
Persistent cookies are deleted from the application of the Secure USB Device after your Secure USB Device has been removed but they remain on your computer or portable device after the browser is closed and (for example to remember your user preferences next time you use the Private eBanking service).

Session cookies are used to enhance the security of the Private eBanking service.

Persistent cookies are used to provide you with certain functionality. For example, to remember choices you make (such as your user name, language or the region you are in), or to recognise the computer or portable device from which you access a site, and to provide enhanced and more personal features. These cookies are not used to track your browsing outside of the eBanking service.

The table below lists the cookies used by the Private eBanking service. These cookies are used for both the Secure USB Device and other devices unless indicated otherwise.

The Private eBanking service is not offered without the use of these cookies. If you do not consent to the use of these cookies, you should remove the Secure USB Device (where cookies are stored on the Secure USB device) or, where cookies are stored on the App on your portable device, delete the App from your portable device as this will prevent us from reading the cookies.

Session Cookies

Cookie Name	Source	Purpose	Comment
AL_SESS	Airlock	Session tracking	
BRSINFO_browser	Browser	security: anti-phishing. tracking browser changes	Customer Client+LoginApp
BRSINFO_cpuInfo	Browser	security: anti-phishing. tracking browser changes	
BRSINFO_env	Browser	security: anti-phishing. tracking browser changes	Customer Client+LoginApp Contains concatenated details of date + javaEnabled +windowSize
BRSINFO_os	Browser	security: anti-phishing. tracking browser changes	Customer Client+LoginApp
BRSINFO_osPlatform	Browser	security: anti-phishing. tracking browser changes	Customer Client+LoginApp Contains concatenated details of the plugins installed in the user's browser
BRSINFO_screenColorDepth	Browser	security: anti-phishing. Tracking browser changes	Customer Client+LoginApp
BRSINFO_sysLang	Browser	security: anti-phishing. tracking browser changes	Customer Client+LoginApp
BRSINFO_portalApp	PortalApp	security: anti-phishing. tracking browser changes	Not used for Secure USB Device

Persistent Cookies

Cookie Name	Source	Purpose	Comment
CLX_EB_LOGIN_INFO	LoginApplication	Stores preferred language and tenant	Used by the login application webserver to ensure that the login page appears the same as it did when the user previously logged in Not used for mobile device
CLX_MB_LOGIN_LANG	LoginApplication	Stores preferred language	Language MobileBanking Not used for Secure USB Device or tablet device
CLX_MB_LOGIN_ <bank>_<session_id>	LoginApplicaiton	Simplified Login with Binding Cookie	Not used for Secure USB Device or table device