

# PRIVACY AND COOKIES POLICY

---

## | Privacy Policy: Personal data protection charter

Data protection within Société Générale Luxembourg applies to all personal data processed by it under the conditions set out in our applicable Terms and Conditions and the Personal Data Protection Policy ci-dessous.

When you use the Private eBanking service, we may automatically collect and store certain information in server log files including, but not limited to, IP addresses, Internet Service Provider (ISP), browsing data, browser type and language, pages opened and closed, and dates or date stamps, which we use for internal reporting and review purposes.

Private eBanking is used via an app installed on your mobile device (smartphone tablet), and we may collect the following additional information about you from this app:

### ***(I) Disclosed information***

Information you provide when filling in an electronic or paper form. This includes information disclosed at the time of registration for using the application.

### ***(II) Additional information***

If you contact us, we may keep track of this correspondence.

### ***(III) Information on devices***

We may gather information about the device or computer that you use to download or send a copy of the application on your mobile device, including, if available, unique identifiers of the mobile device, operating system, browser type, mobile network information, and device phone number for system administration purposes. We may associate this type of information on the device with the Disclosed information and process the combined information as personal data for the duration of their combination.

### ***(IV) Information on location***

If you use the Private eBanking service with a mobile device, this may help us identify your location and we may collect and process information about it. When you access the Private eBanking service with a mobile device, your personal data may be required for accessing some of this service's features. If you wish to use these special features, you will be asked to accept the use of your personal data for this purpose. You may withdraw your consent at any time in the application preferences.

## | Cookies Policy

This cookies policy explains our limited use of cookies and of the information gathered by cookies within the Private eBanking service. By using the Private eBanking service, you consent to the use of cookies referred to in this cookie policy. We use cookies and the information they gather only to deliver service features and improve the security of the Private eBanking service. If you cease to use the Private eBanking service, we will no longer read the cookies, or use the information they collect. However, cookies cannot be disabled when using the Private eBanking service.

### **1. What are cookies and how are they used?**

Cookies are text files containing small amounts of information downloaded to your computer or mobile device when you visit a website or other Internet service. On your next visit to the web domain of origin, cookies are returned to this domain, which therefore has access to the data stored in the cookies. This enables a website or web-based service to recognise the computer or mobile device from which you access the website or service, and store the choices you make (user name, language or region).

When you access the Private eBanking service from a computer, cookies are saved in your browser; when you access Private eBanking from a mobile device (smartphone, tablet), they are stored in the application you download to that device.

### **2. Why do we use cookies?**

Identifying your computer or mobile device and storing your preferences enables us to provide you with custom features, and allows you to browse efficiently, improving the overall user experience.

Identifying when log in and log out of Private eBanking also enables us to take steps aimed at improving security when you use the Private eBanking service.

### **3. What types of cookies are used?** *Session cookies and persistent cookies*

Session cookies are deleted automatically when you shut your browser.

Persistent cookies are deleted after logging out, but remain on your computer or mobile device after the browser is closed (to remember your preferences the next time the Private eBanking service is used).

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

Persistent cookies are used to provide you with certain features, for example, remember your choices (username, language or region), recognise the computer or mobile device from which you access the Private eBanking, or provide you with enhanced and customised features. These cookies are not used to track your browsing outside of the eBanking service.

The table below lists the cookies used by Private eBanking.

The eBanking service is not available without the use of these cookies. If you do not consent to the use of these cookies, you must set up your browser accordingly or, if cookies are stored on the application on your mobile device, you should delete the application from your mobile device to prevent us from reading cookies.

CookieName	Source	Purpose	Comments
AL_SESS	Airlock	Session tracking	
BRSINFO_browser	Browser	Security: anti-phishing. tracking browser changes	CustomerClient+LoginApp
BRSINFO_cpuInfo	Browser	Security: anti-phishing. tracking browser changes	CustomerClient+LoginApp
BRSINFO_env	Browser	Security: anti-phishing. tracking browser changes	CustomerClient+LoginApp. Contains concatenated details of date + javaEnabled + windowSize.
BRSINFO_os	Browser	Security: anti-phishing. tracking browser changes	CustomerClient+LoginApp
BRSINFO_osPlatform	Browser	Security: anti-phishing. tracking browser changes	CustomerClient+LoginApp
BRSINFO_Plugins	Browser	Security: anti-phishing. tracking browser changes	CustomerClient+LoginApp. Concatenated details of the plugins installed in the user's browser.
BRSINFO_screen	Browser	Security: anti-phishing. tracking browser changes	CustomerClient+LoginApp. Contains concatenated details of screen width + screen height + screen colour depth
BRSINFO_screenColorDepth	Browser	Security: anti-phishing. tracking browser changes	CustomerClient+LoginApp
BRSINFO_sysLang	Browser	Security: anti-phishing. tracking browser changes	CustomerClient+LoginApp
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