

Privacy Policy

EFG Hermes KSA

Entity Name and Activity

EFG Hermes KSA ("the Company") is a leading financial services company providing investment services, asset management, securities brokerage, and investment banking to individual investors, corporate clients, and financial institutions within and outside Saudi Arabia. We are committed to protecting your Personal Data in accordance with the Personal Data Protection Law issued by Royal Decree No. M/19 dated 09/02/1443H and its Implementing Regulations.




Contact Information and Update Record

Contact Information	Details
Department	Data Protection
Address	Laysen Valley, Tower 9, 3rd Floor, King Khalid Road, Postal Code 12329, Riyadh, Kingdom of Saudi Arabia.
Phone	009660112938048
Email	data.protection@efg-hermes.com
Website	www.efghermesksa.com
SDAIA License No.	3250001427
Data Protection Officer	
Name/Title	Mohamed Al Qassim - Data Protection Officer
Email	data.protection@efg-hermes.com

Update Record:

Date	Version & Changes
May 2024	Version 1.0 - Initial Privacy Policy
March 2026	Version 2.0 - Comprehensive update to align with SDAIA Privacy Policy Guidelines (Version 1.0 - August 2024). Updated response timeframes per Article 12 of the Implementing Regulations. Enhanced data lifecycle details and cross-border transfer safeguards.
July 2026	Version 2.1 – Updating company address

Personal Data to Be Collected

Data Category	Details
 Account Data	Full name • National ID/Residency number • Date of birth • Nationality • Mailing address • Phone number • Email address • Employment information
 Financial Data	Bank account information (IBAN) • Income and wealth information • Transaction records • Investment portfolio
 Transaction Data	Order and trade details • Transaction date and time • Transaction value and type

Technical Data	IP Address • Browser type and OS • Cookies • Login and usage logs
Compliance Data	Identity documents (ID/passport copy) • KYC information • AML information • Suitability assessment
Communication Data	Phone call records • Email correspondence • Text messages • Customer service chat logs
Note	Some data is mandatory (identity, basic financial) while other data is optional (marketing preferences).

Collecting Personal Data Methods and Purposes

A. Collection Methods:

Method	Details
Direct Collection	Account opening forms • Service request forms • Trading platforms • Mobile applications • Company website • Phone calls • Personal interviews
Indirect Collection	Cookies and tracking technologies • Web analytics tools • Publicly available information • Credit information providers • Regulatory authorities • EFG group companies

B. Processing Purposes:



- Providing Financial Services: Opening/managing accounts, executing orders, brokerage services, investment advisory
- Regulatory Compliance: KYC implementation, AML compliance, suitability assessment, regulatory reporting, judicial compliance
- Customer Relations: Account communications, inquiry responses, technical support, periodic reports
- Risk & Security: Fraud prevention, system security, risk management
- Improvement: Service enhancement, new product development, platform analytics
- Marketing (with explicit consent): Product information, event invitations, newsletters

Legal Basis for Collection and Processing of Personal Data






Legal Basis	Description
Explicit Consent	Obtained for account opening and marketing. Withdrawable anytime by contacting the DPO.
Contractual Obligation	Necessary to execute the financial services contract (account opening, order execution).
Legal Obligation	Required for: Capital Market Law • AML Law • Personal Data Protection Law • CMA rules • Other regulatory requirements.
Legitimate Interest	To prevent fraud, protect security, manage risks, improve services, and protect legal rights.
Public Interest	When necessary for public interest (cooperating with regulatory/security authorities).
Note	Multiple bases may apply.

Personal Data Processing Lifecycle

- Collection: Collect minimum necessary data • Use secure methods • Obtain consent when required • Ensure clear and direct methods
- Storage: Store in secure systems • Implement strict security • Define access permissions • Maintain integrity and confidentiality
- Use: Use only for specified purposes • Ensure data accuracy • Limit access to authorized employees • No incompatible processing

-  Sharing: Share only with specified entities (Section Seven) • Ensure recipient compliance • Enter data protection agreements • Monitor compliance
-  Destruction: Secure destruction after retention period • Use irrecoverable deletion methods • Document the process

Personal Data Sharing

Entity Type	Entities	Purpose & Frequency
 Regulatory	CMA • SAMA • Ministry of Commerce • Zakat Authority • Criminal Evidence Directorate • Financial Investigation Unit	Regulatory compliance, AML, reporting Frequency: Periodic/continuous
 Service Providers	Tadawul • Edaa • Banks • IT providers • Credit info providers • Auditors • Legal advisors	Transaction execution, settlements, technical services, audit Frequency: As needed
 Marketing Service Providers	Digital marketing services providers (Egypt)	Purpose: Social media, digital marketing, online advertising, PR Frequency: As needed
 EFG Group	EFG Hermes (Egypt, UAE, Bahrain)	Integrated services, operational support, HR records (for EFG employees), providing financial services to clients across EFG Group, analytical reports Frequency: Continuous Safeguards: Binding agreements
 International	Cloud providers • Market data providers • Trading platforms	Data hosting, transaction processing, market data Frequency: Continuous Safeguards: Data processing agreements

 Cross-border Safeguards: Adequate protection in receiving countries • Binding agreements • Encryption • Your consent when necessary • SDAIA compliance. We NEVER sell your data for marketing.

Storage, Retention & Destruction

A. Storage Location:

- Servers in KSA
- Cloud servers with approved providers with appropriate protection
- Data centers with international security standards

B. Retention Periods:

Data Type	Retention Period
 Identity & KYC documents	10 years from the relationship's end
 Transaction records	10 years from the transaction date
 Compliance & AML records	10 years from the relationship end
 Communications	10 years from the communication date

Technical data & logs	10 years from the relationship end
Marketing data	Until consent withdrawal or 10 years from last interaction

Note: Data may be retained longer if legally required or to protect our legal rights.

C. Destruction & Security:

- Destruction Methods: Secure electronic deletion • Data overwriting • Physical destruction • Anonymization • Documented process
- Technical Security: Encryption (SSL/TLS, AES-256) • Firewalls • Intrusion detection • Multi-factor authentication • 24/7 monitoring
- Administrative Security: Security policies • Employee training • Confidentiality agreements • Periodic risk assessments
- Organizational Security: Need-to-know access • Separation of duties • Audit logs • Incident reporting procedures

Your Rights

Right	Description & Exercise Method
Right to Be Informed	Know how data is collected, legal basis, processing, storage, destruction, and disclosure entities. Access your information through the means added in this Policy or contact us.
Right of Access	Request access via: Online platforms • Customer service • Written request to DPO Response: 30 days (extendable to 60 with notice if extra effort required)
Right to Copy	Request data copy in clear, readable format Method: Email Data.protection@efg-hermes.com or account portal Response: 30 days (extendable to 60)
Right to Correction	Request correction of inaccurate/incomplete data Method: Online account or customer service Response: 30 days with notification
Right to Destruction	Request destruction when: Data no longer necessary • Consent withdrawn • Unlawful processing • Legal requirement Note: May not be possible if legally obligated Response: 30 days
Right to Withdraw Consent	Withdraw consent anytime unless another legal basis exists Method: Contact DPO at Data.protection@efg-hermes.com or 009660112938048 Does not affect prior lawful processing
Right to Complain	File complaint with SDAIA if dissatisfied
Important	No fees required • Identity verification may be requested • All response times per Article 12 of Implementing Regulations

Complaint Filing Mechanism

Level	Contact Information
Company Level	Department: Data Protection Email: data.protection@efg-hermes.com Phone: 009660112938048 Address: Laysen Valley, Tower 9, 3rd Floor, King Khalid Road, Postal Code 12329, Riyadh, Kingdom of Saudi Arabia. Website: www.efghermesksa.com Processing: 30 days with status updates
SDAIA (if unsatisfied)	Authority: Saudi Data & AI Authority Website: https://sdaia.gov.sa/ar/default.aspx Platform: https://dgp.sdaia.gov.sa/wps/portal/pdp/home Address: Northern Ring Road, Al Nakheel Dist, Riyadh, KSA

Policy Access and Updates

Access Methods:

We are committed to making this Privacy Policy accessible to all Data Subjects in clear, non-misleading, and easy-to-read language. You can access this Policy through:




-  Company website: www.efghermesksa.com/privacy-policy
-  Email upon request: Data.protection@efg-hermes.com

Language Availability:

This Privacy Policy is available in both Arabic (العربية) and English. In case of any conflict between the Arabic and English versions, the Arabic version shall prevail.

Update Notifications:

We will notify you of any material changes to this Privacy Policy through the following channels:

-  Prominent notice on our website homepage
-  Email notification to your registered email address
-  Text message (SMS) to your registered phone number

You will have [30 days] to review changes before they take effect unless immediate implementation is required by law.

Periodic Review:




We conduct periodic reviews of this Privacy Policy to ensure:

- Compliance with the latest regulatory requirements and SDAIA guidelines
- Alignment with industry best practices
- Accuracy and completeness of information provided
- Clarity and readability for all user categories

Any amendments or updates are recorded in the Update Record table in Section Two above.

Relevant policies and documents:

For more information, please refer to:

-  Cookie Policy (Cookies)
-  Saudi Personal Data Protection System
-  Executive regulations of the personal data protection system