

Privacy policy

Privacy policy

1. Introduction	2
2. Who this privacy policy applies to	3
3. How we collect your personal data	4
4. What personal data we collect and use	5
5. Why we use your personal data	9
6. Who we share your personal data with and why	12
7. What automated decisions we make	15
8. How long we keep your personal data for	15
9. Transfers outside the UK and the EEA	16
10. Direct marketing – including your right to opt out	16
11. Cookies and similar technologies	16
12. How we keep your data secure	18
13. Your rights	18
14. Updates to this policy	19
15. Contact us	19

Introduction

Your privacy is important to us. The purpose of this privacy policy is to explain how we use (or 'process') your personal data so that you understand what we do with it, why we use it, who we share it with, the circumstances in which we'll share it, the steps we'll take to keep it secure, the options available to you and your rights. When we say 'you' or 'your' in this privacy policy, we mean any of the people listed in section 2.

This privacy policy applies to any products or services you have with Marcus. It continues to apply even if you stop using our products and services or if our agreement to provide you with such products and services comes to an end. You should read it alongside the terms and conditions for the product or service you have with us.

About us

When we use 'we', 'us' or 'Marcus' in this privacy policy, we are referring to Marcus by Goldman Sachs® in the United Kingdom. Marcus by Goldman Sachs is a trading name of Goldman Sachs International Bank (GSIB) in the United Kingdom, and GSIB is the controller of your data.

GSIB is registered in England and Wales, with the company number 01122503. In the UK, GSIB's use of personal data is regulated by the Information Commissioner's Office.

Whenever we refer to our 'website', we mean marcus.co.uk and any associated websites.

Whenever we refer to our 'mobile app', we mean the Marcus mobile app.

Providing us with accurate information

You are responsible for making sure that any information you give us is accurate and up to date - you must tell us if anything changes as soon as possible. If you believe that the information we hold about you is wrong, incomplete or out of date, you can contact us using the contact details in section 15.

What do we mean by personal data?

Any information that is about you or that can be used to identify you is personal data. This includes your name, email, phone number, personal ID numbers such as your passport or driving licence number, and online or device information like IP addresses.

A list of the personal data that we collect, generate and use is set out in section 4.

2. Who this privacy policy applies to

This privacy policy applies to you if you fall into any of the categories of people listed below - we process personal data about all of them:

- Visitors to our website or social media pages or people who interact with our digital advertisements.
- Anyone who uses our mobile app.
- Anyone who applies for a Marcus account or product.
- Marcus account holders, including joint account holders, and people who have previously held a Marcus account.
- Someone who makes or receives a payment to or from a Marcus account.
- Representatives of a Marcus account holder (such as those holding a valid power of attorney, appointed third parties or executors).
- Callers to our Customer Care Team.
- Anyone who corresponds with us by post, email, social media or any other method.
- Anyone connected to an account holder, such as a relative or close associate ('connected parties').

If you provide information to us about other individuals (such as connected parties), you'll need to direct them to this privacy policy.

We want to make clear that throughout this privacy policy, when we say 'you,' we are referring to individuals acting in their own capacity (for example, an account holder discussing their account with us), as well as individuals providing information about others (for example, a representative of an account holder, or joint account holder, discussing an account with us).

What if you're not covered by this privacy policy?

If you have a different relationship with GSIB or Goldman Sachs that isn't listed above, then please visit goldmansachs.com/privacy-and-cookies to find out more about how your personal data is processed.

3. How we collect your personal data

We collect and process data about you in many different scenarios – these are described in the table below.

We collect personal data about you when:
You apply for, open or operate any Marcus account or product, or where a joint account holder or representative acts on your behalf.
You communicate with us by email, over the phone, by post, through our social media platforms, via your account profile or using any other method. We also record all telephone calls and record the phone number from which the call was received.
You open emails, and if you follow links to our webpages from those emails, we record your interactions.
You visit our website, or use our mobile app, products or services.
You make a payment to or from a Marcus account in your name, or one that you're a representative or payee for. We also record personal data that other banks share with us when processing payments to and from non-Marcus accounts.
You make a complaint or give us feedback. This includes any data you share with us or that we receive as part of our investigation into your feedback or complaint.
We request personal data from third parties, whom we use to check your identity and risk profile. In particular, we use fraud prevention agencies and providers of identity verification checks. These companies may source their data from other third parties.
We search public sources, such as news reports that may link you to fraud, money laundering or crime. We also search public sources to identify politically exposed people using our services. We also search lists of government sanctions and run searches on representatives, payees or other connected parties of the account holder or representative.
We receive personal data from regulators or law enforcement agencies about you. This could happen when you apply for an account, hold an account, represent an account holder or you make a payment to an account.

4. What personal data we collect, generate and use

The type of information we collect and generate about you may differ depending on the product or service we're providing and our relationship with you. The table below provides further details. It is always up to you to decide whether to provide us with your personal data, however in some circumstances we won't be able to open or maintain your account if you fail to provide certain information.

Data we collect, generate and use	When we collect it
<p>Contact information</p> <p>This includes titles, names, addresses (including address history), email addresses and phone numbers.</p> <p>Usually we only collect information you provide to us but we'll verify some contact details with third parties.</p>	<p>When you apply for an account or communicate with us by phone, by email, by post or through our website , mobile app or social media pages.</p>
<p>Data used to verify your identity</p> <p>This includes information such as your full name, date of birth, address, National Insurance number, passport or driving licence details, or details from any other identity documents you provide us with.</p> <p>Usually we only collect information you provide to us but we'll verify some identity data with third parties.</p>	<p>When you apply for an account, or when you're an account holder or payee.</p>
<p>Employment status and line of business</p> <p>This includes your income range.</p>	<p>When you apply for an account, or when you're an account holder.</p>
<p>Your source of funds</p>	<p>When you apply for or hold an account with us, in certain circumstances as we deem necessary.</p>
<p>Your relationship with an account holder</p>	<p>When you contact us, or act, on behalf of an account holder.</p>

Data we collect, generate and use	When we collect it
<p>Tax information</p> <p>This includes your tax residency and if applicable, your tax identification number.</p>	<p>When you apply for or hold an account with us.</p>
<p>Your linked account details</p>	<p>When you apply for an account or when you're an account holder.</p>
<p>Account activity information</p> <p>This includes information about your relationship with us, including the products and services you use, your transactions and your ways of interacting with us.</p>	<p>When there is any activity on your Marcus account.</p>
<p>Call recordings and correspondence</p>	<p>When you write to us by post, email, social media or any other method, and when you call us.</p>
<p>Complaints information</p> <p>This includes details about your complaint, and the progress and outcome of your complaint.</p>	<p>Whenever you make a complaint by phone, by email, by post or through our website, mobile app or social media pages.</p>
<p>Device and location information</p> <p>This includes your IP address and approximate geographic location, information about the device or software you use to access our services, and about your browser.</p>	<p>When you visit our website, use our mobile app, apply for an account, log into your account via our website or mobile app or contact us for help or troubleshooting information or when you open or interact (e.g. click on hyperlinks) with operational and/or marketing emails sent by us.</p>
<p>Authentication details</p> <p>This includes login credentials such as your email address and password, PIN or other data we need to secure your access to your account or to verify your identity.</p>	<p>When you visit our website, apply for an account, log into your account via our website or mobile app or contact us.</p>

Data we collect, generate and use	When we collect it
<p>Identification and anti-fraud data</p> <p>This includes any information about you that's linked to your name, addresses, phone number, email address, devices or bank accounts that help us build up a profile of you.</p> <p>We'll use this to check your application or to ensure that your use of our services is genuine. This information is provided to us by you and third parties, including fraud prevention agencies.</p>	<p>When you apply for an account or when you're an account holder.</p>
<p>Information about products or services you have shown an interest in</p>	<p>When you visit our website, use our mobile app apply for an account or hold or manage an account with us or when you open or interact (e.g. click on hyperlinks) with operational and/or marketing emails sent by us.</p>
<p>Social media</p> <p>This includes any information posted or published on our social media pages, like Twitter, Facebook or LinkedIn. We'll also collect information when you communicate with us using these social media platforms.</p>	<p>When you visit or contact us through social media pages.</p>
<p>Tracking technology information</p> <p>This includes information from cookies and similar technologies we use.</p>	<p>When you visit our website, use our mobile app or login to your account or when you open or interact (e.g. click on hyperlinks) with operational and/or marketing emails sent by us.</p> <p>See section 11 for more information on the cookies and similar technologies we use on our website and our mobile app and in our operational and/or marketing emails.</p>
<p>Communications information</p> <p>This includes details of the channels (for example, post and email) you have opted into to receive direct marketing and other communications from us.</p>	<p>When you apply for an account or when you are an account holder.</p>

Data we collect, generate and use	When we collect it
<p>Due diligence and compliance data</p> <p>This includes information from investigations we conduct such as due diligence checks, sanctions and anti-money laundering checks and information collected and used for our other regulatory and compliance checks. We sometimes collect this information from publically available sources.</p>	<p>When you apply for an account and for as long as you hold an account with us.</p>

Sensitive data

Some sensitive types of personal data have special status under data protection law, and we can only use them in specific circumstances. Details of the main types of sensitive data we process and when we collect them are set out in the table below.

Sensitive data we collect and use	When we collect it
<p>Health information</p> <p>This includes details about particular health or disability requirements that you want us to be aware of, so we can help you make use of our services.</p> <p>If this applies to you, we will provide you with more information at the relevant time.</p>	<p>When you share this information with us on the phone, by email, by post, or through our website or social media pages.</p>
<p>Political opinions, religious or philosophical beliefs</p> <p>Sometimes we may become aware of your political opinions and religious or philosophical beliefs. This can happen when we verify your identity, or during our anti-fraud, money laundering and financial crime checks.</p> <p>We conduct these checks in line with our legal and regulatory obligations. We use this personal data for reasons of substantial public interest (including to comply with legal and regulatory obligations), or for the establishment, exercise or defence of legal claims.</p>	<p>When you apply for an account, or when you're an account holder.</p>

Sensitive data we collect and use	When we collect it
<p>Criminal offences information</p> <p>This includes criminal offences or criminal records that we become aware of. This can happen when we verify your identity, or during our anti-fraud, money laundering or financial crime checks, including from public information.</p> <p>If we identify certain types of criminal activity, we may not be able to offer you our services.</p>	<p>When you apply for an account, make a payment, and when you're an account holder.</p>

5. Why we use your personal data

We'll only use your personal data where we have a lawful reason to do so – we've set out the lawful reasons for using your data below.

To meet our legal obligations

We use your personal data to help us comply with the relevant laws and regulations that apply to us and our products and services, including laws and regulations which relate to:

- the provision of retail banking services;
- anti-money laundering, terrorist financing and the prevention and detection of unlawful acts and criminal activity;
- consumer protection;
- third party access (for example, in relation to powers of attorney); and
- taxation.

To fulfil our contract with you

When you become a Marcus customer we agree to provide you with certain services. We will use your personal data where it is necessary for us to meet the obligations in our contract with you, such as to apply interest payments, facilitate payments to and from your account and produce annual statements.

When using your data is necessary for our legitimate interests

This means that we use your personal data where it is within our legitimate interests to do so. For example, it is in our legitimate business interests to analyse how you interact with our services and emails so that we can continue to develop and improve our website, mobile app and products.

We won't use your personal data where your own interests, fundamental rights or freedoms override our interests to use it. In certain circumstances when we are relying on our legitimate interests to process your personal data, you have the right to object to us using it – see section 13 for more details. The table below includes details of our legitimate interests to use your personal data, but in each case we may have other legal reasons for using it, for example, to meet our legal obligations or to fulfil our contract with you.

It is necessary for our legitimate interests to use your personal data to do the following:

Conduct all necessary checks that help us to comply with the law and manage our risks appropriately, including verifying your identity so we can open an account for you.

Communicate with you, respond to any correspondence and contact you when we need to provide you with information about our services.

Maintain the security of your account and our services.

Protect you, us and third parties against fraud, money laundering and crime, and to investigate circumstances of suspected fraud.

Understand, maintain and improve the performance of our business and its systems, operations, products, services, operational and marketing emails by tracking your use of them through data analytics, models and algorithms;

Providing functionality in our website and mobile app as well as testing new systems and checking upgrades to existing systems.

Analyse market trends and user preferences to test and evaluate our existing products, and research potential new services.

Help train our staff so that we can maintain the quality of our products and services.

Fulfil our regulatory obligations and business requirements by keeping records of calls, correspondence and our business activities and archiving and backing up data.

Produce management information and reports to help us identify potential issues, and to ensure we are managing our risk appropriately. This includes assessing, monitoring and managing financial, reputational and other risks, conducting audits of our business, liaising with our regulators, protecting data used by our business and establishing, enforcing and defending against legal claims.

Meet and provide evidence that we comply with UK law and regulations and the laws and regulations of the countries where our GSIB affiliates are located. This includes performing ongoing compliance checks, account and transaction monitoring, transaction reporting, tax reporting and responding to requests from public authorities, tax authorities and law enforcement agencies, including to help detect and prevent crime.

Deliver targeted advertising online. More details about this can be found in section 11 or you can find out more by clicking on the cookies preferences link on our website or the cookie settings section in our mobile app.

When you have provided your consent

We will occasionally ask for your specific consent to process your personal data. For instance, we directly market some products and services to you by post or email if you have provided consent for us to do so. You can give or withdraw this consent at any time – see section 10 for further details.

Please note that this does not affect the lawfulness of our processing of your data carried out with your consent before the withdrawal. If you withdraw your consent, we may not be able to provide you with certain products and services. If this applies to you, we will provide you with more information at the relevant time.

For other reasons

When we receive information about your health or disability requirements, we may use it to support you by making adjustments to our services and to protect your best interests, including your economic well-being. We will only process such information where we are lawfully permitted to do so.

If you do not want us to process information concerning your health or disability requirements, you can raise an objection and we will consider your request – see section 13 for further details.

We may also process your personal data for the establishment, exercise or defence of legal claims, where it is in the substantial public interest, where it is necessary to protect your or another person's life or where authorised by law.

6. Who we share your personal data with and why

We share your personal data with other members of the Goldman Sachs group and with third party service providers, who act on our instructions and on our behalf to help provide you with our products and services. We only share your data where it is lawful to do so and it will only be shared and used for the reasons listed in section 5 and as described below. Some third parties who we share your data with process it as independent controllers in their own right in accordance with their own privacy policies, for example credit reference agencies and the UK Financial Services Compensation Scheme.

Why we share your data	Who we share it with
<p>To provide services to you, such as processing payments you make and to fulfil our contractual obligations to you.</p>	<p>Banks, anyone who acts as a payee on an account and third party service providers.</p> <p>We may also share your data with any joint account holders and with third parties that we communicate with on your behalf, such as your representatives</p>
<p>To help detect, investigate and prevent fraud, money laundering or crime.</p>	<p>Law enforcement agencies, fraud prevention agencies and third party service providers who may share it with others for the same reason.</p>
<p>When we're required to do so by law, or when we're asked to respond to requests from law enforcement agencies or regulators.</p>	<p>Law enforcement agencies, government, regulators, courts, dispute resolution bodies and tribunals, under applicable laws of any relevant jurisdiction and parties appointed by our regulators to carry out investigations and audits.</p>
<p>To protect the funds in your account(s).</p>	<p>The UK Financial Services Compensation Scheme</p>
<p>To verify your identity.</p>	<p>Credit reference agencies and third party services providers.</p>
<p>To verify your linked bank account, your device, phone number and email address. This is to make sure they belong to you and aren't being used for fraud, money laundering or financial crime.</p>	<p>Fraud prevention agencies and risk management companies.</p>

Why we share your data	Who we share it with
<p>If our business, or part of it, is sold or reorganised, including any transfer or potential transfer of any of our rights or duties under our agreement with you.</p>	<p>Prospective or actual purchasers or transferees and their advisors.</p>
<p>We may need to share your data with tax authorities to comply with both UK and international obligations.</p>	<p>HMRC and tax authorities in other countries, who may share your data with other authorities.</p>
<p>Other extenuating circumstances, such as litigation or asserting or defending our legal rights and interests or if we need to get legal advice.</p>	<p>Any other person or company we reasonably think we need to. For example, with our legal advisors.</p>
<p>To send direct marketing messages to you.</p>	<p>Any third parties which provide marketing services to you on our behalf.</p>
<p>To analyse how you use our services, our mobile app and interact with our emails.</p>	<p>Analytics and marketing vendors acting on our behalf.</p>
<p>For market research purposes and to identify customer trends.</p>	<p>Market research agencies acting on our behalf.</p>
<p>If you have given us instructions to share your data.</p>	<p>Anybody else that we've been instructed to share your information with, either by you, a joint account holder or anybody else who provides instructions or operates any of your accounts on your behalf.</p>
<p>Other reasons that we'll explain at the appropriate time and always with your consent.</p>	<p>The third parties who ask for your data, who we'll tell you about when we ask for your consent.</p>

Credit reference agencies

We use the credit reference agencies (CRAs) Experian and Equifax and TransUnion to verify your identity. When CRAs receive a search from us, they will place an identity search footprint (also known as a 'soft footprint') on your credit file. This identity search footprint cannot be seen by other financial institutions or banks.

We'll continue to exchange information about you with CRAs while you have a relationship with us. However, we do not carry out checks with CRAs to find out your creditworthiness. To find out more about how CRAs use your information including how your data is shared and your data protection rights with them, visit:

Experian - experian.co.uk/crain

Equifax - equifax.co.uk/crain

TransUnion - transunion.co.uk/legal/privacy-centre

Fraud prevention agencies

We share your data with fraud prevention agencies which use it to verify your identity and help prevent fraud, money laundering and financial crime. We do this to comply with the laws and regulations that apply to us, to meet our contractual obligations to provide our services to you and within our legitimate interests to protect you and our business. They can also share it with third parties for the same purpose, and transfer it outside of the UK and EEA.

Whenever fraud prevention agencies transfer your personal data outside of the EEA, they ensure that those recipients protect your data to the same standard as it's protected within the EEA. They do this through legal contracts. Sometimes they'll also insist that the recipients follow international frameworks for data to be shared securely.

They will receive your:

- contact information
- ID information
- IP address and location
- device and technical details
- information about your relationship with an account holder
- information about your use or interest in our products or services

We share this data when you visit our website, use our mobile app, apply for or hold an account, or if you're a representative on a Marcus account or a close associate or relative of an account holder.

If fraud is detected, you could be refused certain services, finance or employment, including by those third parties who have received your data from fraud prevention agencies. Fraud prevention agencies can hold your personal data for different periods of time, and if you are considered to pose a fraud or money laundering risk, your data can be held for up to six years.

Sometimes we and fraud prevention agencies may allow law enforcement agencies to use your personal data to detect, investigate and prevent crime.

If we, or a fraud prevention agency, think that you pose a fraud or money laundering risk, we may refuse to provide you with our services or financing. We may also stop providing existing services to you. A record of any fraud, money laundering or financial crime risk will be retained by the fraud prevention agencies, and may result in others refusing to provide services, financing or employment to you.

Any decisions about money laundering or financial crime risk are reviewed by the Marcus team.

Sharing aggregated or anonymised information

We may share aggregated or anonymised information within and outside of the Goldman Sachs group of companies with partners such as research groups, data aggregators, universities or advertisers. For example, we may share aggregated information about our account holders' account balances with data pooling service providers to better understand the UK savings market. This information will not identify you as an individual.

7. What automated decisions we make

Sometimes, we use your data (including data we collect from third parties) to make automated decisions about you.

For example, like most banks, when you apply for an account and throughout our relationship with you, we use technology to automatically process data about you including risk scores, your name, addresses, phone numbers, email address, devices or bank accounts to:

- Detect and prevent improper or fraudulent use of our products and services. Our automated systems will alert us to any attempts like this, helping us avoid known risks and detect patterns of behaviour that are consistent with fraud.
- Decide whether to offer you services or products by assessing whether your data or behaviour poses a fraud, money laundering, or financial crime risk. It will check for inconsistencies in data you have previously shared with us or where you appear to have deliberately hidden your true identity, and look for similarities with known fraudulent conduct, money launderers or people committing financial crime.

Our use of automated systems helps us make fair and consistent decisions about you, so we can provide a better quality service and help protect your account and the integrity of our products and services. Our use of automated decisions might also result in your application for an account being declined. If we make a decision like this, you have the right to challenge it. For more information on this, please get in touch with us using the contact details in section 15.

8. How long we keep your personal data

Marcus will keep your data for varying time periods depending on your relationship with us and the status of that relationship. When determining how long to keep your data, we take into account our legal and regulatory obligations as a bank and our legitimate interests (such as, preventing fraud, responding to regulatory, supervisory or ombudsmen enquiries, and establishing, exercising or defending legal claims, disputes or complaints).

If you have a Marcus account, we will keep your information for as long as the account is open and for a further 8 years after its closure (and in some cases for longer, but only if we have a lawful basis to do so). If you submit an application for a Marcus account but do not accept the relevant terms and conditions to become a customer, we will keep your information for 12 months (or in some cases for longer, but only if we have a lawful basis to do so).

| 9. Transfers outside the UK and the EEA

We transfer your personal data outside the UK and the European Economic Area (EEA) to provide our products and services. For example, as a member of the Goldman Sachs group, we rely on services provided to us by our group companies in the United States, India and elsewhere. Some of our service providers may also process personal data outside of the EEA. In connection with any such transfer, we will comply with applicable data protection laws.

Where recipients of your personal data are located in countries that are outside the UK and EEA and do not provide for the same level of data protection as considered adequate in the UK and European Union, we take appropriate measures to ensure that your data is protected. For example, where required, our service providers and Goldman Sachs affiliates sign standard contractual clauses approved by the European Commission, or other supervisory authorities.

To find out more about our international data transfers and the measures we take to protect your personal data, including how to receive a copy of them, please contact us using the contact details in section 15.

| 10. Direct marketing – including your right to opt out

When you apply for a Marcus account, we ask if you'd like to receive marketing material by email or in the post. You can choose not to receive it.

If you do choose to receive it, you can opt out at any time by logging into your Marcus account, clicking the unsubscribe link in one of our marketing emails (which will unsubscribe you from email marketing only), or by calling our Customer Care Team.

We use technology, including tracking pixels, in our direct marketing emails to detect whether and how you have interacted with them and to analyse email engagement at an aggregated level. To disable tracking pixels, you can change the settings in your email client to block the display or download of external images.

If you unsubscribe or ask us to stop sending marketing, it may take us a short period of time to update our systems to fulfil your request. During this short period, you may continue to receive marketing messages from us.

Even if you don't opt in to receive marketing messages, we will contact you with important information, such as updates to our terms and conditions, your annual statements and information we are required to provide to comply with our legal obligations.

We also deliver targeted online advertising. The choices you make regarding receiving marketing material by post or email will not impact the display of our targeted online advertising. For more information about our targeted online advertising, including how to exercise choice, see section 11 below click on cookie preferences on our website or visit the cookie settings section of our mobile app.

| 11. Cookies and similar technologies

We use cookies and similar technologies on our website and mobile app for performance, security and advertising purposes, which are described below. A cookie is a small file that is stored on your device (such as your mobile phone or PC). Cookies can collect and send data when you visit a website, use an app, interact with online advertisements, refresh a webpage or open and interact with an email. We use the term 'cookies' to include all technologies that work in a similar way including software development kits.

Essential cookies

We use these cookies to make sure our website and mobile app work as quickly and smoothly as possible. They also help us protect your account from fraud and provide you with secure login. We also use them to remember choices that you make on our site and your application information. You cannot turn these cookies off.

Cookies that improve your experience

We use these cookies to display website content and information that's more relevant to you. We also use these cookies to understand your engagement with our mobile app, which helps us improve the in-app experience, content and functionality. These cookies are optional and we'll ask for your consent before storing them on your device. You can change your preferences about these cookies at any time using our cookie preferences tools.

Cookies that help with advertising

We use these cookies to help us tailor our adverts based on things you've interacted with on our website. They allow us to show you adverts we think you'll be interested in on other websites and track how well they work. We don't display adverts from other companies on our website.

Advertising cookies from third parties (such as Facebook and Twitter) allow us to share data with the operators of those websites and with service providers. We, or they, may use those cookies to better understand your interests and to deliver and manage targeted advertising.

These cookies are optional and we'll ask for your consent before storing them on your device. If you don't turn them on, you may still see our adverts on other sites but they won't be tailored to you. You can change your preferences about these cookies at any time using our cookie preferences tool.

Your cookie preferences

Our website and mobile app both have cookie preferences tools that allow you to make choices about optional cookies at any time.

To open our website cookie preferences tool, click on the cookie preferences link, which is displayed in the footer on every page of our website. This tool allows you to enable or disable optional cookies on our website.

If you change your cookie preferences when you are on certain pages of our website, such as an application page, your changes will only be stored when you proceed to another page or refresh the current one.

The cookie preferences tool in our mobile app is found in the cookie settings section. This tool allows you to enable or disable optional cookies that are used both in our mobile app and on the pages of our website accessed via the app.

If you change your cookie choices using our app preferences tool within the mobile app's cookie settings section, some of your choices will only take effect when you close and re-open the app.

Your cookie choices will only impact and be saved on the device you use to make your choice. We will not sync your cookie choices across the different devices you may use to access your Marcus account online.

12. How we keep your data secure

Marcus takes the security of your personal data seriously and provides training and education about privacy and data security to all our staff. We seek to limit access to your personal data to authorised employees, agents, contractors or vendors. We have also implemented physical, electronic and procedural measures designed to protect your data from loss and destruction as well as unauthorised access, disclosure and alteration.

If you have a concern about the security of your account, our website, or our mobile app please visit our security page marcus.co.uk/security. We encourage security professionals to practice responsible disclosure and let us know right away if a vulnerability is discovered on our website or mobile app. We will investigate all legitimate reports and follow up if more details are required. Goldman Sachs has engaged with HackerOne to manage all submissions. You can submit the vulnerability report at this link: <https://hackerone.com/goldmansachs>.

13. Your rights

We've set out your rights in relation to your personal data below. If you have any questions about your rights or you wish to exercise any of your rights, please contact us using the contact details set out in section 15. If you have a Marcus Community account, you can access, delete and correct the data which is associated with it and held in the Marcus Community through the Marcus Community website. If you wish to exercise other rights relating to the Marcus Community data, please contact us using the contact details set out in section 15. You should understand that your rights do not apply in all circumstances and are subject to exceptions.

Access

You have the right to be provided with information about the personal data we have about you and details of how we use it, as well as the right to receive a copy of such personal data.

Rectification

You have the right to request that we rectify your information if it is incomplete or inaccurate. If your personal data changes, we encourage you to let us know or change the information yourself in your account profile. You can also ask us to update incorrect or incomplete information.

Erasure (right to be forgotten)

You have the right to request that we erase your personal data in certain circumstances. We may continue to store your personal data if we are entitled or required to retain it.

Restriction of processing

You can request that we restrict use of your personal data in certain circumstances. There may be situations where we are entitled to continue using your information and/or to refuse your request.

Data Portability

In certain circumstances, you may have the right to request a copy of the personal data that we hold on you in a commonly used format, so you can pass it to a third party, or, where technically possible, to have us transmit such data directly to a third party. You may have this right if we are using your data based on your consent or our contractual obligations with you and if we are using an automated method to process it.

Object

In certain cases, we use your personal data where it is necessary for our legitimate interests to do so (see section 5 for more information). When this is the case, you have the right to object, on grounds relating to your particular situation, to us using your personal data in this way. There may be situations where we are entitled to continue processing your personal data and/ or to refuse your request.

Withdrawal of consent

Where we rely upon your consent to use your personal data, you have the right to withdraw consent at any time. This does not affect the lawfulness of the processing of your data carried out with your consent before the withdrawal.

Complaints

If for any reason you're not satisfied with our approach to using your personal data, you have the right to complain to the regulator. Our regulator is the Information Commissioner's Office, who can be contacted at ico.org.uk/global/contact-us.

14. Updates to this policy

The information in this privacy policy may change from time to time. For example, the categories of personal data that we collect, the reasons it's used and the ways in which it's shared may change.

We will update this privacy policy to reflect these changes wherever necessary and we'll give you notice of any significant changes. This privacy policy was last updated at the date noted at the end of this document.

15. Contact us

If you have any questions or concerns about how we use your data, please get in touch with us.

You can call our Customer Care Team on 0800 085 6789. Our lines are open Monday to Friday, from 8am to 8pm.

You can write to us at:

Marcus UK
PO Box 74787
London
EC4P4JP

You can also contact our Data Protection Officer at privacymarcusUK@gs.com.

If you would like this privacy policy in another format such as large print or Braille please contact us.