

J.P.Morgan

WORKPLACE SOLUTIONS

Workplace Solutions Privacy Notice

Effective Date: 24th October 2024



WHO IS THIS PRIVACY NOTICE ISSUED BY AND WHAT INFORMATION DOES IT PROVIDE?

J.P. Morgan Workplace Solutions (“Workplace Solutions”) is a brand name for equity compensation administration business conducted by Global Shares and other financial products and services offered through J.P. Morgan Securities LLC and other affiliates of J.P. Morgan Chase & Co.

The purpose of this Privacy Notice (“Notice”) is to explain how we “process” or use your personal data, to help you understand why we collect, use, store, share and secure your data, and to explain your privacy rights.

The Notice is issued by Workplace Solutions and its branches, subsidiaries and affiliates identified as the parties responsible for determining the means and the purposes of processing your personal data, listed in SCHEDULE A, (you can access this section by clicking [here](#) if you are viewing the document electronically). In this Notice, we use “Workplace Solutions” “we”, “us” or “our” depending on context.

This Notice uses certain defined terms:

“Personal data” is information that is about any individual, or from which any individual is identifiable. It can be anything from your name to your IP address. You can see what personal data we collect in section ‘What Personal Data do we collect, generate and use?’ or, by clicking [here](#) if viewing this document electronically. Please de-identified or aggregation information, is not considered personal data and therefore is not subject to this Notice.

“Process, processed or processing” encompasses the collection, use, storage and analysis of data. The principle covers anything that is done with any personal data, whether or not by automated means.

This Notice is designed to supplement any specific terms and conditions which may be applicable to your relationship with us. If you have any questions about this document and how it applies to your personal data, please contact us directly using the details below. Depending on your relationship with Workplace Solutions, other Notices may be made available to you.

This Notice relates to the processing of personal data by Workplace Solutions. To the extent you have a relationship with other J.P. Morgan affiliates, we would encourage you to review the privacy notices issued by those affiliates for further details of how they may process your personal data.

WHO SHOULD READ THIS NOTICE?

This Notice is addressed to people with whom we interact. This includes:

- visitors to our websites (our “Sites”);
- representatives of customers (including prospective customers, our customers’ advisors, family, office staff or other individuals associated with our corporate clients);
- Users* of the Participant Portal platform who have a share dealing account with us (“Share Account”)
- prospective Users
- vendors
- anyone who calls our service centres or writes to us via post, email or social media, and
- other recipients of our services (together, “you”).

* Users refers to individuals who have a Share Account with Workplace Solutions on the Participant Portal Platform. For Users, additional processing activities will be carried out on behalf of your employer to administer your employee share scheme. This includes Workplace Solutions receiving information about eligible participants to set-up User Share Accounts, providing participation reports and other regulatory scheme information from Workplace Solutions relating to the administration of your employee share scheme. Your employer, as a separate and independent controller of your personal data, is responsible for providing you with a privacy notice on how your personal data is processed for these activities; Workplace Solutions will only process your personal data on the instructions of your employer and in accordance with your employer share scheme rules.

HOW WILL WE UPDATE THIS NOTICE?

This Notice may be amended and updated from time to time to reflect changes such as the categories of data that we collect, process and share or to reflect any changes in applicable law. We encourage you to regularly check this page, and we will include the effective date in order to help you check whether or not there have been any changes since you last accessed the Notice.

WHAT SHOULD I DO IF I HAVE ANY QUESTIONS?

If you have any comments, questions or concerns that are not addressed in this Notice you can contact us through the regular channels, or the following central contacts:

- You can contact our Data Protection Officer at EMEA.Privacy.Office@jpmchase.com or via post at JPMC, EMEA Privacy, JPMorgan Chase Bank, National Association, 18th Floor, 25 Bank Street, Canary Wharf, London E14 5JP, UK.
- Workplace Solutions Privacy Office at privacy.global.shares@jpmorgan.com

OUR APPROACH TO DATA PROTECTION

Data Security: we have implemented appropriate technical and organizational security measures designed to protect your personal data. We protect your data in line with our global security program built on our core principles of only using the data required for the processing in question, controlling access to systems and datasets to those who need to use the data, and using an encryption and anonymization process to secure the data that we hold in our systems. You are responsible for ensuring that any personal data that you send to us are sent securely.

Data Accuracy: we take reasonable steps designed to ensure that any personal data that we process are accurate and, where necessary, kept up to date and that any of your personal data that we process that is inaccurate (having regard to the purposes for which they are processed) are erased or rectified without delay. From time to time, we may ask you to confirm the accuracy of your personal data.

Data Minimisation: we take reasonable steps designed to ensure that your personal data that we process are limited to the personal data reasonably required in connection with the purposes set out in this Notice.

HOW DO WE COLLECT PERSONAL DATA?

We collect personal data in a number of different ways. This table sets out the methods by which we collect your personal data, with some examples.

HOW WE COLLECT PERSONAL DATA	EXAMPLES
When you provide us with personal data	<ul style="list-style-type: none">• When you activate your Share Account.• When you communicate with us via email (or any other electronic channels), phone call, letter or other means• If you contact us, make a complaint or provide feedback, including any data that you share with us or that we receive as part of our investigation into your complaint or feedback
When you use our services	<ul style="list-style-type: none">• Transactions on your account, such as instructing a trade or payment.
From third parties who provide it to us	<ul style="list-style-type: none">• If we carry out checks via credit reference agencies.• Your current or former employer, for example, as part of the share scheme administration process or should we need to confirm your employment status.• Third party sources such as business contacts.• If we engage third parties such as vendor(s) to provide data to us, for example, in connection with the services we provide to you and/or to conduct research.• Government and law enforcement authorities

When you visit or use any of our Sites, for example, Participant Portal	<ul style="list-style-type: none">• When you give us your details to activate your Share Account• When visiting a Site, your device and browser may automatically disclose certain information (such as device type, operating system, browser type, browser settings, IP address, language settings, dates and times of connecting to a Site and other technical communications information).
Social media and publicly available data sources	<ul style="list-style-type: none">• Public social media profiles such as LinkedIn• Search engine results and news reports from available sources including Google, Bloomberg and the Financial Times.• Any public entry on electoral registers, company registers or local equivalents.

Although your provision of personal data to us in connection with this Notice is voluntary (unless we inform you otherwise), we may be unable to provide you with our products/ services (or any part thereof) or comply with any applicable laws or regulations or guidelines and codes issued by regulatory or other authorities if you do not do so.

HOW DOES THIS NOTICE APPLY TO THIRD PARTY PERSONAL DATA?

If you transfer third party personal data to us this Notice will also apply to that personal data.

If you supply us with the personal data of third parties, you will be responsible for informing those third parties that their personal data has been transferred to us and for informing them that this Notice will apply. You are also responsible for the collection and recording of their consent, if necessary.

In addition, if such personal data is considered confidential under applicable law, you are responsible for ensuring that the third parties have waived any applicable confidentiality requirements.

WHEN DO WE RECORD OUR INTERACTIONS WITH YOU?

In some circumstances, and as permitted by applicable law, we will record, monitor and retain communications (including but not limited to facsimile, telephone conversations, email, instant messaging, your interaction with our Sites and any other electronic communications) including those held between you and employees of Workplace Solutions. These records and recordings are made for the purposes of ensuring compliance with Workplace Solutions' legal and regulatory obligations and internal policies.

All such records will be the sole property of Workplace Solutions and will be accepted by you as conclusive evidence of the orders, instructions or conversations recorded, if applicable.

In connection with the records held in relation to activities relating to the reception, transmission and execution of orders, a copy of the recording of our conversations and communications with you will be available to you and/or any competent supervisory authority, upon request, for a period specified by applicable law, which may vary depending on your jurisdiction.

WHAT PERSONAL DATA DO WE COLLECT, GENERATE AND USE?

This table sets out the categories of personal data that we collect and generate. The type and amount of data that we collect and generate will differ depending on your relationship with us, and the services that we provide to you.

PERSONAL DATA COLLECTED, GENERATED AND USED	EXAMPLES
Personal details	<ul style="list-style-type: none"> • Your name, including any previous names, preferred names, or nicknames. • Your gender, date of birth, nationality, residency, tax residency and marital status. • Information concerning your identity, such as government issued tax identification numbers, government issued number e.g., Social Security Number. • Information about your lifestyle and social circumstances and details of your education and qualifications. • Authentication data, such as your login details. • Photographs and visual images, such as CCTV footage if you visit our offices or images of identity documents obtained during onboarding. • Information relating to your behaviour, such as how you interact with our services.
Contact details	<ul style="list-style-type: none"> • Your address, telephone number, email address, and social media details.
Employment details	<ul style="list-style-type: none"> • The nature of your industry and current role and position, plus any other business activities. • The names of your current and former employers. • Any contact details relating to your work. • Your share scheme eligibility and allocations, transaction history.

Financial details	<ul style="list-style-type: none"> • Your bank account number, account holder name and details. • Your instruction records, transaction details, and counterparty details. • Your assets and financial position. • The fact that you have a banking relationship with another member of the Workplace Solutions and/or J.P. Morgan group.
Views and opinions	<ul style="list-style-type: none"> • Any views and opinions about us that you choose to send to us or make public.
Electronic Identifying Data	<ul style="list-style-type: none"> • IP addresses, geolocation data, online identifiers (including in relation to your device) and cookies. • Data relating to your use of our sites, mobile app or Participant Portal platform, such as browsing activity or transaction logs.
Personal data of third parties	<ul style="list-style-type: none"> • Any of the above in relation to other parties such as family members, dependants, friends, employees and advisors.
Others	<ul style="list-style-type: none"> • Any other personal data we receive from you (or on your behalf), including voice recordings or files (e.g., documents, audio files or video files) received via electronic communication channels.

Subject to and to the extent provided under applicable law, certain personal data is deemed Sensitive (“Sensitive Personal Data”). If we collect Sensitive Personal Data, as noted below, we will only process it for specific purposes.

EU GDPR and UK Data Protection Act 2018: race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sexual life, any criminal offenses, genetic or biometric data or any other information that may be deemed to be sensitive.

California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020: certain government identifiers (such as SSN, driver’s license,

passport number); an account log-in, financial account, debit or credit card number with any required security code, password, or credentials allowing access to an account; precise geolocation (which means within 1,850 feet of a particular person); contents of mail, email, and text messages; genetic data; biometric information processed to identify an individual; information concerning an individual's health, sex life; sexual orientation; or information about racial or ethnic origin, religious or philosophical beliefs, or union membership.

The table below sets out some examples of when we might process Sensitive Personal Data.

SENSITIVE PERSONAL DATA COLLECTED, GENERATED AND USED	EXAMPLES
Race or ethnicity	We may request this information from you when you apply for one of our services, and subsequently process this information for the purposes of a legal obligation, e.g., diversity reporting.
Political opinions and religious or philosophical beliefs	You may agree to share your beliefs with us or make them public. Alternatively, we may become aware of them during the administration of your account when we carry out checks required for the detection and prevention of crime, or if necessary for the establishment, exercise, or defence of legal rights.
Criminal offences	We may become aware of criminal history during our financial crime checks, such as anti-fraud procedures and anti-money laundering checks, including information received from public sources. We will process this data in connection with our legal obligations and for the detection and prevention of crime.

Health information	You may tell us your health information to ensure that you can use our services, such as any dietary requirements that you may have. We may also request this information from you when required by law or if it is in our legitimate interest to provide a safe and secure environment at our premises.
Biometric data	We may request this information from you when you apply for or login to one of our services or, we need to carry out checks such as Know Your Client checks e.g., face recognition, and for detection and prevention of crime.
Sensitive Personal Data of third parties	Any of the above in relation to other parties such as family members, dependants, friends, employees, and advisors.

SELLING AND SHARING OF PERSONAL DATA

Workplace Solutions does not sell or share personal data with respect to California residents, as those terms are used in the California Privacy Rights Act of 2020.

WHEN DO WE SHARE PERSONAL DATA WITH THIRD PARTIES?

We will share your personal data in some circumstances, such as with other members of the Workplace Solutions and/or J.P. Morgan group and third-party service providers who act on our instructions under legal agreements to assist us in providing our products and services. We may also share your data with some third parties which process it in their own right and in accordance with their own privacy policies. Examples of third-party companies include service providers for electronic signatures. You should be aware that once your data is shared with third parties they

may also be under a legal or regulatory duty to share that information, in some cases by making that data public, in certain jurisdictions.

WHO WE SHARE YOUR DATA WITH	EXAMPLES
Other entities within the Workplace Solutions and/or J.P. Morgan group	<ul style="list-style-type: none"> • We may share your personal data for our internal operational purposes, for example in connection with our anti-money laundering obligations. • We may share your personal data that we processed for the purposes of Know Your Client checks if you wish to purchase products and services from another member of the Workplace Solutions and/or J.P. Morgan group. • In limited circumstances and subject to appropriate controls, we may share your personal data with other members of the Workplace Solutions and/or J.P. Morgan group in order to assess whether or not some of their products and services are suitable for you or to market products and services to you.
To your Employer	<ul style="list-style-type: none"> • We may share your personal data with your employer where it is necessary for the employer administration of their employee share scheme.
Third party service providers who provide services to us, including their subcontractors or delegates	<ul style="list-style-type: none"> • We may share your personal data with payment services providers, where we need to do so in order to satisfy a payment request that you make. • If we hold your assets in custody as part of the services that we provide, we may share your data with third party companies who support the market infrastructure. • We may share your personal data with data aggregation services if you choose to use them, or if it is in our legitimate interests to do so. • To analytics and search engine providers that assist us in the improvement and optimisation of our website.

	<ul style="list-style-type: none"> • We may share information with other service providers in order to assist them in complying with their legal obligations, such as Know Your Client checks. • We may share your personal information with relevant communication or social media channel providers or platform hosting service providers if you choose to use them, or if it is in our legitimate interest to do so.
Workplace Solutions' professional advisors	<ul style="list-style-type: none"> • We may share personal data with our accountants, auditors, financial advisors, lawyers and other outside professional advisors.
Third party plug-in providers	<ul style="list-style-type: none"> • Our Sites may use third party plug-ins or content. If you choose to interact with any such plugins or content, your personal data will be shared with the third-party provider of the relevant social media platform. We recommend that you review that third party's privacy policy before interacting with such plug-ins or content.
Any relevant third-party acquirer(s)	<ul style="list-style-type: none"> • If we sell or transfer all or a portion of our business or assets. • If we reorganise, dissolve or liquidate all or a portion of our business or assets.
Governmental, legal, regulatory, or similar authorities	<ul style="list-style-type: none"> • If they require us to share your personal data. • If we are required to report any actual or suspected breach of applicable law or regulation. • Any relevant party to the extent necessary for the establishment, exercise or defence of legal rights. • Any relevant party for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Other third parties	<ul style="list-style-type: none">• Any relevant party to the extent necessary for the establishment, exercise or defence of legal rights.• Any relevant party for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.• Where you have provided your consent for social engagement or networking purposes, introducing you to other individuals who have a relationship with J.P. Morgan and disclosing your contact details to them.
---------------------	--

SHARING YOUR PERSONAL DATA INTERNATIONALLY

Because of the international nature of our business, we may need to transfer your personal data within Workplace Solutions, the J.P. Morgan group, and to third parties, in connection with the purposes set out in this Notice. For this reason, we may transfer your personal data to other countries that may have different laws and data protection compliance requirements, including data protection laws of a lower standard to those that apply in the country in which you are located.

Where we transfer your personal data to other countries, we do so on the basis of:

- adequacy decisions
- suitable Standard Contractual Clauses; or
- other valid transfer mechanisms

If you want to receive more information about the safeguards applied to international transfers of personal data, please contact us using the details provided in 'WHAT SHOULD I DO IF I HAVE QUESTIONS?' or by clicking [here](#) if you are viewing this document electronically.

HOW LONG DO WE RETAIN YOUR DATA FOR?

We will retain your personal data in line with our data retention policy and for the minimum period required. The duration of the retention period is determined by number of criteria including the nature of our relationship with you, the relevant jurisdiction, the type of data and the products and services that the data relates to.

We will retain your personal data for as long as we have an ongoing relationship with you – for example, whilst you have a Share Account – or where we need to retain the personal data in connection with the purposes set out in this Notice and we are permitted to do so under applicable law. In the event of a legal claim, we may continue to process your personal data for such period as is necessary in connection with that legal claim.

After this period, we will typically retain your personal data for any additional limitation period (i.e., any period during which a legal claim could be raised) plus two months after the end of the limitation period, in order to ensure that the data can be used in connection with any legal claim which may be brought. During the legal hold period we will restrict our processing of your personal data to the storage of, and maintaining the security of, the data, except to the extent that the data needs to be reviewed in connection with any legal claim, or any obligation under applicable law.

Once we no longer need to retain your personal data, we will either:

- permanently delete or destroy the relevant personal data;
- archive your personal data so that it is beyond use; or
- anonymise the relevant personal data.

YOUR LEGAL RIGHTS

Subject to and to the extent provided under applicable law, such as the EU GDPR, the UK Data Protection Act of 2018 and the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020, you may have certain rights in relation to your data and we want to make sure that you can exercise them. In some cases, however, we may not be able to continue to provide you with certain products and services or continue to operate your account.

To exercise one or more of these rights, or to ask a question:

- please contact us using the details provided in 'WHAT SHOULD I DO IF I HAVE QUESTIONS?' or by clicking [here](#) if you are viewing this document electronically.
- If you are a California resident and wish to exercise one or more of your rights, you or someone you authorize to make a request on your behalf may call us at (800) 573-7138 or click on the following link <https://www.chase.com/digital/resources/privacy-security/privacy/ca-consumer-privacy-act/ccpa-request> and follow the instructions provided. Additional detail is available in our Frequently Asked Questions available here: <https://www.chase.com/digital/resources/privacy-security/privacy/ca-consumer-privacy-act/faqs>

Your Rights	Description
Access	You have the right to request access to or copies of the personal data that we process or control, together with information regarding the nature, processing and disclosures of that personal data.
Rectification	<p>If you believe that the personal data that we process or control is incomplete or inaccurate, you have the right to request rectification.</p> <p>If you believe that the personal data is inaccurate, you have the right to ask us to restrict its processing while it is being verified.</p>
Erasure	<p>You have the right to request that we delete your personal data if:</p> <ul style="list-style-type: none"> • We no longer need the personal data for the purposes for which it was processed or collected; • We originally requested your consent to process the personal data, but you wish to withdraw your consent; or • We are not processing your personal data lawfully; in which case you may request that processing is restricted instead.

Restriction	You have the right to request that we restrict the processing of your personal data as mentioned above, or alternatively if we no longer need the personal data for the original purpose, but you require the personal data for the establishment, exercise or defence of legal claims.
Data Portability	Under some circumstances, you have the right to receive your personal data in a readable format. You may also, under certain circumstances, request that we send your personal data in a readable format to a third party; note that we will not be responsible for how that third party processes your personal data and you should ensure that you are comfortable with the contractual terms or privacy arrangements that they have in place.
Objection	You have the right to object, on grounds relating to your particular situation, to the processing of your personal data by us or on our behalf.
Consent	If we have asked for your consent in order to process your personal data, you have the right to withdraw that consent.
Automated Processing	<p>You have the right to request information about the existence of and an explanation of the logic involved in, the significance of and any envisaged consequences of any automated processing of your personal data that has a legal effect or a significant effect on you.</p> <p>You have the right not to be subject to a decision based solely on automated processing. This right shall not apply where the processing is necessary for a contract with you, or the processing is undertaken with your explicit consent, or the processing is authorised by law.</p>
Complaints	You have the right to complain to the appropriate Data Protection Authority regarding the processing of your personal data, either by us or on our behalf.

HOW WE USE COOKIES ON OUR SITES

A cookie is a small file that is placed on your device when you visit a website (including our Sites). It records information about your device, your browser and, in some cases, your preferences and browsing habits. We may process your personal

data through cookie technology, in accordance with our Cookie Policy <https://www.globalshares.com/GS-Cookie-Notice-2023.pdf>

We will analyse the cookie data collected by us to improve our Sites and our services to you. The data collected will be stored in our systems and protected with the same degree of security used for all other personal data.

DIRECT MARKETING

We may process your personal data to contact you, primarily by mail and email (and other electronic communication channels) and also on occasion by telephone, so that we can provide you with information concerning products and services that may be of interest.

If you do not wish to receive marketing communications from us you can opt out at any time by contacting the Service Desk, or by electronically unsubscribing from emails we have sent to you. After you unsubscribe, we will not send you further promotional messages, but we may continue to contact you to the extent necessary for the purposes of any services you have requested.

SCHEDULE A – WORKPLACE SOLUTIONS ENTITIES

For the purposes of this Notice, the relevant Workplace Solutions entities (which may be considered “controllers” under the laws of certain jurisdictions) are:

Workplace Solutions Entity	Contact Details
Global Shares Ireland Limited	West Cork Technology Park, Clonakilty, Cork, Ireland
Global Shares Execution Services Ltd (Malta)	171 Old Bakery Street, Valletta, VLT1455, Malta
Global Shares Inc	1000 North King Street, Wilmington, New Castle County, Delaware 19801, USA
Global Shares Financial Services Inc	1000 North King Street, Wilmington, New Castle County, Delaware 19801, USA

If you are unsure as to which J.P. Morgan Chase & Co. entity is collecting or processing your personal data (or, under the laws of certain jurisdictions, the “controllers” of your personal data), please contact us using the details provided in section ‘WHAT SHOULD I DO IF I HAVE QUESTIONS?’ or by clicking [here](#) if you are viewing this document electronically.

SCHEDULE B - PURPOSES FOR WHICH WE MAY PROCESS YOUR PERSONAL DATA, AND LEGAL BASES FOR PROCESSING

The purposes for which we may process personal data and subject to and to the extent provided under applicable law, the legal basis on which we may perform such processing are as follows:

PROCESSING PURPOSE	LEGAL BASIS FOR PROCESSING
<p>Anti-Money Laundering / Know Your Client checks:</p> <p>Fulfilling our regulatory compliance obligations, including ‘KYC’ checks; and confirming and verifying your identity (including by using credit reference agencies); and screening against government, supranational bodies (including but not limited to the European Union and the United Nations Security Council) and/or law enforcement agency sanctions lists, as well as internal sanctions lists and other legal restrictions.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purposes of preventing money laundering, sanctions violations and protecting against fraud (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary – it is not used for processing that is necessary or obligatory in any way).

<p>Account activation and administration:</p> <p>Information required to open and administer accounts includes, without limitation, the ultimate beneficial ownership, personal identification details or, for legal entities, country of citizenship, residence, or address of record, documentation requested by us for the purposes of conducting Know Your Client and anti-money laundering and counter terrorism financing identification and verification and any information relating to tax status.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of onboarding new clients (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary – it is not used for processing that is necessary or obligatory in any way).
<p>Provision of products and services to you:</p> <p>Management of accounts and related services, including Notification of any tasks and the performance of tasks necessary for the provision of the requested services including managing payments and trade requests; communicating with you in relation to those services.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of providing products and services to you (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary – it is not used for processing that is necessary or obligatory in any way).

<p>Marketing and promotion activities:</p> <p>evaluating whether the products and services of Workplace Solutions and/or the J.P. Morgan group, may be of interest to you and providing you with marketing information concerning such products and services, by mail, e-mail, SMS, social media, post, telephone or in person, unless you have specifically instructed us not to do so, and subject to ensuring that such communications are provided to you in compliance with applicable law; maintaining and updating your contact information where appropriate.</p>	<ul style="list-style-type: none"> • We have a legitimate interest in carrying out the processing for the purpose of conducting marketing and prospecting (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary – it is not used for processing that is necessary or obligatory in any way).
<p>Operation of our Sites:</p> <p>operation and management of Workplace Solutions mobile apps and websites; providing content to you; displaying advertising and other information to you; and communicating and interacting with you via our app and sites.</p>	<ul style="list-style-type: none"> • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of operating our Sites (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary – it is not used for processing that is necessary or obligatory in any way).

<p>IT operations: management of our communications systems; operation of IT security; and IT security audits.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of managing and operating our IT systems and ensuring the security of those systems (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
<p>Health and safety: health and safety assessments and record keeping; and compliance with related legal obligations.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • We have a legitimate interest in carrying out the processing for the purpose of providing a safe and secure environment at our premises (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • The processing is necessary to protect the vital interests of any individual.
<p>Financial management: sales; finance; corporate audit. and vendor management.</p>	<ul style="list-style-type: none"> • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of managing and operating the financial affairs of our business (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary – it is not used for processing that is necessary or obligatory in any way).

<p>Research:</p> <p>conducting market or customer satisfaction research; and engaging with you for the purposes of obtaining your views on our products and services.</p>	<ul style="list-style-type: none"> • We have a legitimate interest in carrying out the processing for the purpose of conducting research and producing analysis (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary – it is not used for processing that is necessary or obligatory in any way).
<p>Security:</p> <p>physical security of our premises (including records of visits to our premises and CCTV recordings); and electronic security (including login records and access details, where you access our electronic systems).</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • We have a legitimate interest in carrying out the processing for the purpose of ensuring the physical and electronic security of our business, premises, and assets (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
<p>Investigations:</p> <p>detecting, investigating and preventing breaches of policy, and criminal offences, in accordance with applicable law.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • We have a legitimate interest in carrying out the processing for the purpose of detecting, and protecting against, breaches of our policies and applicable laws (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
<p>Legal compliance:</p> <p>compliance with our legal and regulatory obligations under applicable law.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation.

<p>Legal proceedings: establishing, exercising and defending legal rights.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • We have a legitimate interest in carrying out the processing for the purpose of establishing, exercising or defending our legal rights (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
<p>Improving our products and services: identifying issues with existing products and services; planning improvements to existing products and services; and creating new products and services.</p>	<ul style="list-style-type: none"> • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of improving our products or services (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary – it is not used for processing that is necessary or obligatory in any way).
<p>Risk Management: Audit, compliance, controls and other risk management.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • We have a legitimate interest in carrying out the processing for the purpose of managing risks to which our business is exposed (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).

<p>Fraud prevention:</p> <p>Detecting, preventing and investigating fraud.</p>	<ul style="list-style-type: none">• The processing is necessary for compliance with a legal obligation; or• The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or• We have a legitimate interest in carrying out the processing for the purpose of detecting, and protecting against, fraud (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or• We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary – it is not used for processing that is necessary or obligatory in any way).
--	---