

WALKERS PROFESSIONAL SERVICES ('WPS')**GLOBAL PRIVACY STATEMENT FOR CLIENTS, WEBSITE USERS, AND BUSINESS CONTACTS****1. INTRODUCTION AND PURPOSE**

This Privacy Statement sets out in detail the manner in which Walkers Professional Services and its affiliated entities (together, "**WPS**", "we", "us" or "our") collect, use, disclose, transfer and otherwise process personal information. Your privacy is important to us, and we are committed to protecting and safeguarding your rights.

This Privacy Statement is provided in accordance with applicable data protection and privacy legislation, including but not limited to:

- the UK General Data Protection Regulation and Data Protection Act 2018 ("**UK GDPR**");
- Regulation (EU) 2016/679 ("**EU GDPR**");
- the Cayman Islands Data Protection Act (2021 Revision);
- the Bermuda Personal Information Protection Act 2016 ("**PIPA**");
- the Hong Kong Personal Data (Privacy) Ordinance (Cap. 486);
- the Data Protection Regulations applicable in the Dubai International Financial Centre ("**DIFC**") and Abu Dhabi Global Market ("**ADGM**"); and
- any other applicable laws governing the processing of personal information in the jurisdictions in which WPS operates (together, "**Data Protection Laws**").

This Privacy Statement is intended to ensure transparency as to how your personal information is processed and to facilitate the exercise of your rights.

2. SCOPE AND APPLICATION

This Privacy Statement applies to personal information relating to:

- users of WPS websites and social media pages;
- clients and prospective clients (including individuals and representatives of corporate clients);
- beneficial owners, directors, officers, trustees, settlors, protectors and beneficiaries of structures administered by WPS;
- professional advisers, intermediaries and counterparties; and
- business contacts.

This Privacy Statement does not apply to employee or recruitment data, which is covered under separate notices.

3. DATA CONTROLLER AND ACCOUNTABILITY**3.1 Controller status**

Each WPS entity processes personal information as a data controller in respect of the personal information processed in connection with its activities.



WPS operates a global service delivery model. personal information is processed and shared between WPS entities in accordance with an intra-group data sharing and transfer agreement which:

- governs the allocation of roles and responsibilities;
- ensures compliance with applicable Data Protection Laws; and
- incorporates appropriate safeguards for international transfers.

Further information on each WPS entity can be found in **Section 18 Contact Information**.

3.2 Sharing with Walkers Global Law Firm

In certain circumstances, WPS may share your personal information with Walkers Law Firm where this is necessary to provide you with an effective and appropriate service. In such cases, Walkers Law Firm will act as an independent data controller in respect of your personal information. For further information on how Walkers Law Firm collects, uses, and protects your personal information, please refer to their privacy statement [here](#).

3.3 Joint controllers

Where that information is collected and sent to other organisations for processing that is in both our and their interests, we will be making decisions together in relation to that particular processing and will be 'joint controllers' with the organisations involved. As joint controllers, we and the other organisations involved in making these decisions will be jointly responsible to you under data protection laws for this processing. In other circumstances, the organisation receiving your information will be separately responsible to you and use your personal information in the ways described in its privacy statement (and not ours).

See **Section 9 Disclosure of Personal Information** for further details.

4. CATEGORIES OF PERSONAL INFORMATION

WPS processes the following personal information appropriate to the nature of its services.

4.1 Online information

- information that you submit via our contact forms on the website and any correspondence we have with you over email or phone;
- your social media handle, any information you post on our social media pages or posts in which you include a hashtag or mention relating to us and information regarding your activities on our social media pages generally (for example, the time and date of your posts);
- technical information about your visit, including details of your visits to the Website and your navigation around the Website, traffic data, communication data, information about the device you use to access the Website, your Internet protocol (IP) address used to connect your computer to the Internet, your login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform;
- information concerning your engagement with our social media content, including likes, shares, comments, reactions, clicks, impressions and audience interaction statistics;
- we automatically collect information about how visitors use our website by using cookies and similar technologies if, where they are not essential to make the website work, you have consented to their use. The data we collect automatically includes information, such as your IP address, pixel ID, device type, unique device identification number, browser type, operating system, broad geographic location and other technical information. Collecting this information enables us to better understand the visitors who come to our Website, where they come from and what content on our website is of interest to them. To learn more about how we use cookies and how to switch them off please see our [Cookies Policy](#);
- Marketing preferences and when you have interacted with emails.



4.2 Identification and contact data

- name, title, date of birth, nationality, residential and correspondence addresses, email addresses and telephone numbers.

4.3 Corporate and relationship data

- directorships, shareholdings and ownership interests, roles, authorities and signing powers, relationships between entities and individuals.

4.4 Due diligence and KYC data

- identity documentation, proof of address, source of wealth and funds, professional and financial background information.

4.5 Financial and transactional data

- bank account details, fee and billing records, asset ownership information.

4.6 Regulatory and compliance data

- AML risk ratings, sanctions/PEP screening results, regulatory filings and correspondence.

4.7 Communications data

- emails, correspondence, instructions, meeting notes, board documentation, extra information that you choose to tell us.

4.8 Professional and business information

- employer, job title, professional qualifications, business contact details, professional affiliations, professional interests and areas of expertise, and information obtained from commercial business directories and intelligence providers.

4.9 Event and visitor information

- event registration details, attendance records, dietary or accessibility requirements that you choose to provide to us, and visitor and meeting records.

5 SOURCES OF PERSONAL INFORMATION

We collect personal information from a variety of sources in the course of providing our services. These include personal information obtained directly from data subjects, as well as information received from clients and intermediaries acting on their behalf. We collect personal information from publicly available sources, regulatory bodies and governmental authorities, and third-party due diligence providers. We may also obtain personal information from commercial business information providers, marketing databases, lead generation providers, event organisers, professional networking platforms and corporate intelligence providers. Such information may include business contact details, professional roles, employer information, areas of interest and other information relevant to identifying prospective clients or business contacts. In addition, personal information may be collected through interactions with our website, including through the use of cookies and similar technologies.

We ensure that any collection of personal information is limited to what is necessary, proportionate, and relevant for the specific purposes for which it is processed, in accordance with Data Protection Laws.



Where personal information is required to comply with legal or regulatory obligations, or is necessary for the performance of a contract or to enter into a contract with WPS, you are required to provide such information.

Failure to provide the requested personal information may result in WPS being unable to establish or continue a relationship with you, provide services, or comply with its legal and regulatory obligations.

Where personal information is not obtained directly from you, WPS will process such information in accordance with the lawful bases described in this Privacy Statement and will take reasonable steps to ensure that you are informed of such processing in accordance with applicable Data Protection Laws.

6 PURPOSES OF PROCESSING AND LEGAL BASIS

WPS processes personal information for the purposes described below. The legal basis or equivalent legal justification for processing will depend on the jurisdiction concerned and the nature of the processing. Where the UK GDPR or EU GDPR applies, the relevant lawful basis is identified below. In other jurisdictions, WPS relies on the corresponding legal grounds available under applicable Data Protection Laws, including the performance of contractual obligations, compliance with legal and regulatory requirements, reasonable and legitimate business purposes, protection of rights and interests, and other lawful grounds recognised under applicable legislation

In order to enhance transparency and provide a clear and structured overview of how personal information is processed, WPS has included the tables below setting out its principal categories of processing activities.

6.1 Client Onboarding and KYC / CDD

Activity	Description
Purpose of processing	To identify and verify clients and associated persons; to comply with AML/CFT and regulatory obligations
Categories of data subjects	Clients; directors; shareholders; UBOs; trustees; beneficiaries; intermediaries
Categories of personal information	Identification data; contact data; identity documents; source of wealth/funds; screening results
Lawful basis	Legal obligation; contract; substantial public interest
Sensitive data	Criminal conviction data (AML), limited special category data where necessary
Recipients	WPS entities; AML/KYC providers; regulators; professional advisers
Transfers	WPS entities; screened third-party providers

6.2 Provision of Corporate and Fiduciary Services

Activity	Description
Purpose	Provision of corporate administration, fiduciary, trustee and governance services
Data subjects	Clients; directors; officers; authorised signatories; beneficial owners
Data categories	Corporate roles; governance data; communications; financial data
Lawful basis	Contract performance; legitimate interests
Recipients	WPS group; legal advisers; auditors; counterparties
Transfers	WPS entities



6.3 Anti-Money Laundering Monitoring and Ongoing Due Diligence

Activity	Description
Purpose	Ongoing monitoring of clients for AML/CFT and sanctions compliance
Data subjects	Clients and associated persons
Data categories	Screening results; risk scores; transaction data (where applicable)
Lawful basis	Legal obligation; public interest
Recipients	Regulators; AML vendors; law enforcement
Transfers	External screening platforms

6.4 Regulatory Reporting (CRS, FATCA, Economic Substance)

Activity	Description
Purpose	Compliance with tax transparency and regulatory reporting obligations
Data subjects	Clients; UBOs; controlling persons
Data categories	Identification data; tax IDs; ownership structures
Lawful basis	Legal obligation
Recipients	Tax authorities; regulators
Transfers	Cross-border reporting to authorities

6.5 Client Relationship Management and Communications

Activity	Description
Purpose	Managing relationships; responding to queries; identifying prospective clients, maintaining business development records, managing referral relationships and developing professional networks; attendance at events; understanding whether you have interacted with emails; sending you information via newsletters; meetings you have had with us; communicating with you and providing mandatory service communications such as billing reminders and terms and conditions of engagement;
Data subjects	Clients; business contacts; intermediaries
Data categories	Contact data; communications; interaction records
Lawful basis	Contract; legitimate interests
Recipients	WPS group entities
Transfers	Global CRM systems

6.6 Marketing and communications

Activity	Description
Purpose	Sending legal updates, insights, invitations and service-related communications; identifying prospective clients and business contacts; building and maintaining marketing and business development databases; profiling organisations and professional contacts to determine whether WPS services may be relevant to them; managing event invitations and professional relationship activities.
Data subjects	Business contacts; clients; prospective clients
Data categories	Contact details; marketing preferences; interaction data



Lawful basis	Legitimate interests (maintaining relationships, business development and marketing activities), consent where required by applicable electronic marketing laws, and compliance with legal obligations relating to marketing preferences and suppression records.
Recipients	Marketing service providers; CRM tools; social media platforms
Transfers	International email and CRM systems

6.7 Business Development and Prospect Relationship Management

Activity	Description
Purpose	Identifying prospective clients and business opportunities; maintaining business development databases; managing referral networks; maintaining records of interactions with prospective clients and business contacts
Data subjects	Prospective clients; business contacts; intermediaries; professional advisers
Data categories	Contact details; professional information; employer details; business interests; interaction records
Lawful basis	Legitimate interests
Recipients	WPS entities; CRM providers; business intelligence providers

6.8 Website Operation and Analytics

Activity	Description
Purpose	Website operation, security, analytics, audience measurement, advertising performance measurement, content optimisation, marketing attribution and audience development.
Data subjects	Website visitors
Data categories	IP address; device data; usage data; cookies
Lawful basis	Legitimate interests; consent (for non-essential cookies)
Recipients	Analytics providers; hosting providers
Transfers	Cross-border hosting infrastructure

6.9 IT Systems, Security and Fraud Prevention

Activity	Description
Purpose	Ensuring system security, detecting fraud, maintaining IT infrastructure
Data subjects	Users; clients; employees (limited overlap)
Data categories	Login data; system logs; device identifiers
Lawful basis	Legitimate interests; legal obligations
Recipients	IT providers; cybersecurity providers
Transfers	Cloud infrastructure

6.10 Legal and Dispute Management

Activity	Description
----------	-------------



Purpose	Managing disputes, litigation, investigations and regulatory inquiries
Data subjects	Clients; counterparties; witnesses
Data categories	Case records; communications; evidence
Lawful basis	Legal claims; legal obligation
Recipients	Courts; regulators; law firms
Transfers	Jurisdiction-dependent

6.11 Corporate Transactions and Business Reorganisation

Activity	Description
Purpose	Mergers, restructurings, acquisitions or business transfers
Data subjects	Clients; business contacts
Data categories	Corporate and relationship data
Lawful basis	Legitimate interests
Recipients	Advisers; counterparties
Transfers	Cross-border where relevant

6.12 Additional Processing Purposes and Legal Bases

We may use and process your personal information as set out below where it is necessary for us to carry out these activities. Before relying on legitimate interests, WPS considers and balances its interests against the rights and freedoms of the individuals affected and implements safeguards designed to minimise privacy impacts.

Legitimate interests

- To provide you with a more tailored and effective customer service;
- To perform research and analysis aimed at improving our products, services and technologies;
- To undertake market analysis and research (including contacting you with surveys) so that we can better understand you as a customer and provide tailored offers, products and services that we think you will be interested in;
- To tailor the marketing information we send based on information we hold about you;
- Operating social media accounts, engaging with users, reviewing platform analytics, measuring audience engagement and promoting WPS services;
- To identify potential clients, develop professional relationships and promote WPS services to organisations and individuals who may have an interest in those services;
- To identify and record when you have received, opened or engaged with our website or electronic communications;
- To create advertising and other promotional material to publicise our brands and products in marketing campaigns;
- To identify the extent to which your interactions and communications with us or our content contributed to your engagement with us or our brand;



- To administer our websites, applications, social media pages and accounts and our products, and for internal operations, including troubleshooting, testing, training, and statistical purposes;
- For the purposes of corporate restructure or reorganisation or sale or purchase of businesses or assets;
- For efficiency, accuracy or other improvements of our products, services, business processes, databases and systems, for example, by combining systems or consolidating records we hold about you;
- To inform you of updates to our terms and conditions and policies;
- To aggregate or otherwise anonymise your information, and to permit our service providers to do the same, for our or those providers' use of the anonymised information for operational, administrative or business improvement purposes;
- To train, fine-tune, develop and test models which power the artificial intelligence technology we use within our business and in some of our services. For more information, please see the section 'Our use of artificial intelligence.'

Contract

- To facilitate the processing of payments made by you to us, accounting and billing, auditing and identification checking.

Legal Obligation

- We may process your personal information to comply with our legal or regulatory requirements (for example to assist or respond to a request for information from a regulatory body). These requirements include processing to remember your cookie consent preferences for optional cookies used by our website.

Jurisdictional qualifiers

Not all jurisdictions recognised in this Privacy Statement adopt the same lawful basis framework as the UK GDPR or EU GDPR. Where local law applies, references to lawful bases should be read as including the equivalent legal grounds, permissions or conditions for processing under the applicable legislation. WPS will ensure that personal information is processed only where there is a valid legal basis or other lawful justification under the laws applicable to the relevant WPS entity and processing activity.

For example, Certain jurisdictions (including Bermuda) do not recognise "legitimate interests" as a standalone legal basis. In such cases, processing is supported by:

- contractual necessity;
- reasonable business purposes consistent with PIPA requirements; or
- statutory or regulatory obligations.

7 SPECIAL CATEGORY, SENSITIVE, AND CRIMINAL OFFENCE DATA

Where special category data (or equivalent sensitive data) is processed, WPS ensures:

- a valid legal condition applies;
- processing is strictly necessary;
- enhanced controls are implemented.



WPS has included the table below setting out its principal categories of processing activities relating to special category data:

Activity	Description
Purpose of processing	Processing of special category data is carried out only where strictly necessary for the provision of services, compliance with legal and regulatory obligations (including AML/CFT), or the establishment, exercise or defence of legal claims.
Categories of data subjects	Clients; beneficial owners; directors and officers; trustees, settlors and beneficiaries; business contacts where relevant
Categories of special category data	Data revealing racial or ethnic origin (where required for verification); religious or philosophical beliefs (where relevant to fiduciary structures); health data (in limited circumstances); criminal conviction and offence data (for AML/KYC purposes)
Lawful basis / legal condition	Article 9(2)(a) (explicit consent); Article 9(2)(f) (legal claims); Article 9(2)(g) (substantial public interest, including AML); Article 10 (criminal offence data, where authorised by law); plus applicable offshore legal gateways where GDPR does not apply
Necessity and proportionality	Processing is limited to what is strictly necessary for the relevant purpose and is subject to documented assessment, including consideration of less intrusive alternatives
Recipients	WPS entities; AML/KYC providers; regulatory authorities; law enforcement agencies; professional advisors (where necessary)
International transfers	Transfers may occur within the WPS group and to third-party providers located outside the jurisdiction of collection
Safeguards	Enhanced safeguards including: restricted access on a need-to-know basis; segregation of sensitive data; encryption in transit and at rest; contractual protections (including SCCs/intra-group agreements); and heightened confidentiality obligations
Retention period	Retained only for as long as necessary to fulfil the specific purpose, including compliance with applicable legal or regulatory requirements (e.g. AML retention periods)
Key risks and controls	Elevated risk of misuse or unauthorised disclosure mitigated through enhanced technical and organisational measures, periodic access reviews, audit logging and strict internal policies governing use of sensitive data

8 DISCLOSURE OF PERSONAL INFORMATION

Personal information may be disclosed to the following categories of recipients, strictly on a need-to-know basis:

Recipient	Description
WPS Entities	Personal information may be disclosed to other entities within the WPS group of companies located in multiple jurisdictions worldwide where such disclosure is necessary for the efficient delivery of services, group-wide management and administration, compliance with legal and regulatory obligations, and the operation of centralised systems and controls.
Walkers Global Law Firm	Personal information may be disclosed to Walkers Global Law Firm, which operates as a legally separate and independent organisation, where such disclosure is necessary to facilitate the provision of coordinated services to shared clients and to ensure continuity, efficiency and quality in service delivery. This may include circumstances where WPS and Walkers Law Firm act for the



	same or related clients in connection with corporate, fiduciary and legal services. In such cases, each organisation acts as an independent data controller in respect of the personal information it processes. Personal information will only be shared to the extent necessary for the relevant purpose and in accordance with applicable Data Protection Laws. Appropriate safeguards are implemented to govern such information sharing, including data sharing arrangements, confidentiality obligations and (where relevant) contractual and international transfer safeguards.
Professional Advisers	Personal information may be disclosed to professional advisers engaged by WPS or its clients, including lawyers, auditors, accountants and other consultants, where such disclosure is necessary for the provision of services, obtaining legal or professional advice, compliance with regulatory obligations, or the establishment, exercise or defence of legal claims. Such recipients are bound by contractual, professional and/or statutory duties of confidentiality and are required to process personal information only for the authorised purposes.
Business Intelligence and Data Providers	WPS may obtain and supplement business contact information from third-party commercial information providers and business intelligence databases to assist with business development, relationship management, marketing activities and maintaining accurate contact records.
Service Providers (Including IT and Operational Vendors)	WPS engages third-party service providers to support its operations and service delivery. These may include providers of cloud hosting, IT infrastructure, cybersecurity services, document management systems, customer relationship management platforms, KYC and AML verification tools, and payment processing services. Personal information may be disclosed to such providers strictly to the extent necessary for the performance of their services. These providers are subject to contractual obligations requiring them to act only on WPS instructions (where acting as processors), implement appropriate technical and organisational measures, and comply with applicable Data Protection Laws.
Regulators, Authorities and Law Enforcement	Personal information may be disclosed to regulatory bodies, supervisory authorities, tax authorities, courts, tribunals and law enforcement agencies where WPS is required or permitted to do so under applicable law or regulation. This includes disclosures made in connection with AML/CFT obligations, reporting regimes such as CRS and FATCA, court orders, regulatory investigations, or the exercise or defence of legal rights. Such disclosures are limited to what is necessary and proportionate in the circumstances and are carried out in accordance with applicable legal requirements.
Social Media and Marketing Platforms	Where individuals interact with WPS content through digital channels, personal information may be disclosed to social media platforms, marketing service providers and analytics tools for the purposes of communication, engagement, analytics and marketing activities. Such disclosures may occur, for example, where users engage with WPS content, subscribe to communications, or attend events. WPS ensures that appropriate controls are implemented, including the use of configured privacy settings, contractual safeguards and, where applicable, user consent mechanisms in accordance with relevant marketing and data protection laws.

9 INTERNATIONAL DATA TRANSFERS

Given the global nature of WPS operations, personal information is routinely transferred between jurisdictions.

EEA/UK to third country



Your personal information may be transferred outside of the UK and the European Economic Area (EEA) to the third parties described in Sharing your information with third parties.

We want to make sure that your personal information is stored and transferred in a way which is secure. We will therefore only transfer data outside of the UK and EEA where it is compliant with data protection legislation and the means of transfer provides adequate safeguards in relation to your data, for example:

- by way of an intra-group agreement between entities, incorporating the current standard contractual clauses adopted by the European Commission, the UK Information Commissioner's Office or other competent body for the transfer of personal information to jurisdictions without adequate data protection laws;
- by way of a data transfer agreement with a third party, incorporating the current standard contractual clauses adopted by the European Commission, the UK Information Commissioner's Office or other competent body for the transfer of personal information to jurisdictions without adequate data protection laws;
- by transferring your data from entities within the UK and EEA to entities in other jurisdictions by way of a valid international transfer framework;
- by transferring your data to a country where there has been a finding of adequacy by the European Commission, the UK Information Commissioner's Office or other competent body in respect of that country's levels of data protection via its legislation;
- where it is necessary for the conclusion or performance of a contract between ourselves and a third party and the transfer is in your interests for the purposes of that contract; or
- where you have consented to the transfer.

Where we transfer your personal information outside the UK and EEA and where the country or territory in question does not maintain adequate data protection standards, we will take all reasonable steps to ensure that your data is treated securely and in accordance with this Privacy Notice. You can ask to see these by contacting us using the contact details below.

Non-EEA/UK to third country

Where personal information is transferred from other jurisdictions (including, for example, the Cayman Islands, British Virgin Islands, Bermuda, Hong Kong, DIFC and ADGM) to another jurisdiction, WPS ensures that such transfers are carried out in accordance with applicable Data Protection Laws in the relevant jurisdiction.

In particular, WPS will take appropriate steps to ensure that personal information benefits from an adequate level of protection, including, where applicable:

- by entering into intra-group arrangements governing the transfer of personal information between WPS entities, incorporating contractual safeguards and obligations designed to ensure an equivalent level of protection across the WPS group;
- by entering into contractual arrangements with third-party recipients requiring them to implement appropriate technical and organisational measures and to process personal information only in accordance with documented instructions;
- by implementing jurisdiction-specific transfer mechanisms, including those required under local data protection frameworks (such as DIFC/ADGM transfer rules or equivalent offshore requirements);
- by assessing the level of protection in the destination jurisdiction and, where necessary, implementing supplementary safeguards, such as encryption, access restrictions and data minimisation measures;
- where required, by relying on statutory gateways or permitted transfer conditions, including where the transfer is necessary for the provision of services, compliance with legal or regulatory obligations, or for the establishment, exercise or defence of legal claims; and



- where applicable, by obtaining consent or providing appropriate notices in accordance with local legal requirements.

In all cases, WPS will ensure that transfers are limited to what is necessary for the relevant purpose and that appropriate safeguards are applied to protect personal information throughout the transfer and subsequent processing.

10 DATA RETENTION

WPS retains personal information only for as long as is necessary and proportionate having regard to the purposes for which it was collected and processed, the requirements of applicable Data Protection Laws, and WPS's legitimate business and regulatory obligations.

In particular, personal information will be retained for the following purposes:

- **to fulfil the purposes described in this Privacy Statement**, including the provision of corporate, fiduciary, administrative and related services, and the ongoing management of client relationships;
- **to comply with applicable legal and regulatory obligations**, including obligations arising under anti-money laundering and counter-terrorist financing legislation, tax reporting regimes (such as FATCA and CRS), corporate governance requirements, and other applicable statutory or regulatory frameworks; and
- **to enable the establishment, exercise or defence of legal claims**, including the maintenance of records required to respond to disputes, regulatory enquiries, investigations or litigation, and to meet applicable limitation periods.

Retention periods may vary depending on the nature of the personal information, the services provided, the jurisdictions involved, and the applicable legal or regulatory requirements. In determining appropriate retention periods, WPS takes into account:

- the amount, nature and sensitivity of the personal information;
- the potential risk of harm from unauthorised use or disclosure;
- the purposes for which the data is processed and whether those purposes can be achieved through other means; and
- applicable statutory retention requirements and regulatory expectations.

WPS maintains and applies internal data retention policies and procedures designed to ensure that personal information are not retained for longer than is necessary. At the end of the applicable retention period, personal information will be securely deleted, anonymised, or otherwise disposed of in accordance with WPS's internal policies and applicable law.

Retention practices are subject to periodic review to ensure ongoing compliance with applicable Data Protection Laws and to take account of changes in legal, regulatory and business requirements.

11 SECURITY AND CONFIDENTIALITY

WPS implements and maintains appropriate technical and organisational measures designed to ensure a level of security commensurate with the risks associated with the processing of personal information, including the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information.

These measures are designed having regard to the nature, scope, context and purposes of processing, as well as the likelihood and severity of potential risks to individuals. WPS adopts a risk-based approach to information security and applies controls proportionate to the sensitivity of the personal information processed.



In particular, WPS implements measures including:

- **access controls:** the use of role-based access restrictions to ensure that personal information is accessible only to authorised personnel on a strict need-to-know basis, supported by authentication mechanisms and periodic access reviews;
- **encryption and data protection measures:** the use of encryption and other technical safeguards to protect personal information both in transit and at rest, together with measures designed to preserve data integrity and confidentiality;
- **system monitoring and security management:** continuous monitoring of systems, networks and infrastructure to detect and respond to potential security vulnerabilities, unauthorised access attempts or other anomalous activity; and
- **incident response procedures:** the implementation of documented incident management and response processes to ensure that any personal information breach or security incident is identified, assessed, contained, investigated and remediated in a timely and effective manner, including, where required, notification to affected individuals and relevant authorities.

In addition, WPS ensures that:

- personnel handling personal information are subject to confidentiality obligations and receive appropriate training on data protection and information security;
- third-party service providers are subject to contractual obligations requiring the implementation of appropriate security measures; and
- data processing systems and controls are designed to support resilience and the ongoing availability of personal information.

WPS undertakes regular reviews, testing and evaluation of its technical and organisational measures to ensure their continued effectiveness and to address evolving security risks, technological developments and regulatory expectations. Where appropriate, WPS enhances its controls to maintain an appropriate level of protection for personal information.

12 USE OF COOKIES AND TRACKING TECHNOLOGIES

WPS uses cookies and similar tracking technologies on its website to ensure its effective operation, to analyse usage and performance, to enhance user experience and to support the delivery of relevant content.

Where required by applicable law, non-essential cookies are deployed only with your consent, which may be provided and managed through our cookie consent mechanisms. You may withdraw or adjust your cookie preferences at any time via these tools.

We may contact you with targeted advertising delivered online through social media and other platforms operated by other companies, unless you object. You may receive advertising based on information about you that we have provided to the platform or allowed the social media platform to collect using cookies on our Website. You may also receive advertising because, at our request, the platform has identified you as falling within a group whose attributes we have selected as Segments (defined above) or a group that has similar attributes to the individuals whose details it has received from us (or a combination of the two). To find out more, please refer to the information provided in the help pages of the platforms on which you receive advertising from us.

Further information regarding the types of cookies used, their purposes, retention periods and how you can manage your preferences is set out in our [Cookies Policy](#), which should be read in conjunction with this Privacy Statement.

13 SOCIAL MEDIA



We use a number of different social media platforms to communicate with you and to promote products and services. We process your personal information using these platforms in a variety of ways, as follows:

Pages. We use your personal information when you post content or otherwise interact with us on our official pages on Facebook, Instagram, and other social media platforms. We also use the Page Insights service for Facebook and Instagram to view statistical information and reports regarding your interactions with the pages we administer on those platforms and their content. Where those interactions are recorded and form part of the information we access through these Page Insights services, we and the relevant platform are joint controllers of the processing necessary to provide that service to us.

Cookies. We use cookies and similar technologies in our Website to collect and send information to Facebook and Instagram about actions you take on our website and applications. In particular:

- Facebook uses this information to provide services to us and also for further processing for its own business purposes. We and Facebook are joint controllers of the processing involved in collecting and sending your personal information to Facebook using cookies and similar technologies as each of us has a business interest in Facebook receiving this information. You can find out more about these technologies by visiting our cookies policy. The services we receive from Facebook that use this information are delivered to us through Facebook's Business Tools, which include Facebook Pixel, Facebook Social Plugins and Website Custom Audiences. These tools allow us to target advertising to you within Facebook's social media platform by creating audiences based on your actions on our Website and applications and allow Facebook to improve and optimise the targeting and delivery of our advertising campaigns for us;
- We use LinkedIn Insight Tag, a small piece of code that we embed in our websites that allows us to perform in-depth campaign reporting and unlock insights about users that may visit our websites via our LinkedIn campaigns (e.g. by allowing us to discover business demographics by layering LinkedIn data on data about our website visitors). LinkedIn Insight Tag enables the collection of metadata such as IP addresses, timestamps, and events such as page views. You can find out more about these technologies by visiting our [Cookies Policy](#).

Our relationship with Meta and LinkedIn

As we are joint data controllers with these platforms for certain processing, we and each platform have:

- entered into agreements in which we have agreed each of our data protection responsibilities for the processing of your personal information described above;
- agreed that we are responsible for providing to you the information in this privacy notice about our relationship with each platform; and
- agreed that each platform is responsible for responding to you when you exercise your rights under data protection law in relation to that platform's processing of your personal information as a joint data controller.

Meta and LinkedIn also process, as our processor, contact information that we submit for the purposes of matching, online targeting, measurement, reporting and analytics purposes. These services include the processing these platforms carry out when they display our advertisements to you in your news feed at our request after matching contact details for you that we have uploaded to the social media platforms they operate. These advertisements may include forms through which we collect contact information you give to us.

Further information

The Meta company that is a joint data controller of your personal information is Meta Platforms, Inc., 1601 Willow Road, Menlo Park, CA 94025, USA (if you are a UK-registered user) or Meta Platforms Ireland Limited, Block J, Serpentine Avenue, Dublin 4, Ireland (if you are an EEA-registered user). The



LinkedIn company that is a joint data controller of your personal information is LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland For further information regarding these platforms and their use of your personal information, please see:

- Meta's Controller Addendum for Page Insights and UK Controller Addendum for Business Tools (for users located in the UK) and Controller Addendum (for users located in the EEA), and LinkedIn's Page Insights Joint Controller Addendum, which include information which include information regarding how our and these platforms' responsibilities to you are allocated as controllers of your personal information;
- Meta's Privacy Center including its Privacy Policy at <https://www.facebook.com/privacy> and LinkedIn's Privacy Policy which include details of the legal reasons (known as 'lawful bases') on which each platform relies to process your personal information, together with details regarding your data protection rights
- Meta's help pages regarding its Page Insights and Business Tools and its terms and conditions relating to those tools
- LinkedIn's help pages regarding its Page Insights and its terms and conditions relating to its advertising services, including LinkedIn Insight Tag

14 ARTIFICIAL INTELLIGENCE

WPS may utilise artificial intelligence technologies ("AI") as part of its operations and service delivery. AI refers to systems and tools capable of performing tasks that typically require human intelligence, including analysing information, identifying patterns, generating content, and supporting decision-making processes.

How we use AI

WPS may use AI in a controlled and proportionate manner to support and enhance its services and internal operations. This includes, for example:

- assisting with document drafting, review and summarisation;
- supporting research, data analysis and knowledge management;
- enhancing customer relationship management systems and improving operational processes;
- assisting with onboarding, due diligence and administrative functions; and
- improving the efficiency, consistency and quality of internal workflows.

WPS may also use meeting recording, transcription and summarisation technologies to assist with the preparation of meeting records, minutes and related administrative documentation. Such recordings and transcripts are retained only in accordance with applicable retention requirements and internal policies and are subject to appropriate access controls.

AI may therefore be used in connection with any of the purposes described in this Privacy Statement, where appropriate to do so.

Nature of AI use

AI tools may be deployed:

- as part of internally used systems, supporting WPS personnel in carrying out their roles;
- within business processes and operational systems, including client onboarding and management; and
- on a background or assistive basis, to improve efficiency and system functionality.

WPS does not rely on AI to make decisions about individuals without appropriate human involvement.

Safeguards and governance



WPS applies appropriate technical and organisational measures to ensure that AI is used responsibly, fairly and securely. These measures include:

- conducting risk-based assessments prior to deployment of AI tools;
- restricting access to personal information used in AI systems on a need-to-know basis;
- implementing measures to protect confidentiality, including where appropriate data minimisation, anonymisation or pseudonymisation;
- applying contractual and technical controls when engaging third-party AI providers;
- monitoring outputs for accuracy, consistency and potential bias; and
- ensuring appropriate human oversight of AI-supported activities.

Use of personal information in AI systems

Where personal information is processed using AI, such processing will be carried out in accordance with applicable Data Protection Laws and limited to what is necessary for the relevant purpose.

WPS does not use special category data (or equivalent sensitive data) to train AI systems except where there is a clear legal basis and appropriate safeguards are in place.

Where AI tools are provided by third parties, WPS takes steps to ensure that personal information is not used to train or improve such tools unless this is permitted by applicable law and subject to appropriate controls.

Where permitted by applicable law, you may request that your personal information is not used in connection with AI-supported processing by contacting WPS using the contact details provided below, and WPS will consider such requests in accordance with applicable Data Protection Laws and its legal and regulatory obligations.

Automated decision-making

WPS does not carry out solely automated decision-making, including profiling, that produces legal or similarly significant effects on individuals within the meaning of applicable Data Protection Laws.

15 YOUR RIGHTS

You have a number of rights in relation to your information under data protection law. In relation to certain rights, we may ask you for information to confirm your identity and, where applicable, to help us to search for your personal information. Except in rare cases, we will respond to you within one month from either: (i) the date that we have confirmed your identity; or (ii) where we do not need to do this because we already have this information, from the date we received your request.

Data subject right	Description
Right of access	You have the right to request confirmation as to whether we process your personal information and, where that is the case, to obtain access to such data together with certain prescribed information.
Right to rectification	You have the right to request the correction of inaccurate or incomplete personal information held about you.
Right to erasure	In certain circumstances, you may request that your personal information be deleted, for example where it is no longer necessary for the purposes for which it was collected or where processing is no longer lawful.
Right to restriction and objection	You may request that we restrict the processing of your personal information in certain circumstances or object to processing where it is based on legitimate interests or carried out for direct marketing purposes.



Right to data portability	Where applicable, you may request to receive personal information you have provided to us in a structured, commonly used and machine-readable format and to have that data transmitted to another controller.
Right to withdraw consent	Where processing is based on your consent, you have the right to withdraw that consent at any time. This will not affect the lawfulness of processing carried out prior to withdrawal.
Right to raise queries or complaints	You may contact WPS at WPSLegal@walkersglobal.com with any questions, concerns or complaints regarding the processing of your personal information.
Right to lodge a complaint with a regulator	You have the right to lodge a complaint with a relevant supervisory authority in the jurisdiction in which you are located or where the relevant processing has taken place (see list below).

16 COMPLAINTS AND REGULATORS

You are encouraged to contact WPS in the first instance using the contact details provided below. However, you retain the right to contact a relevant supervisory authority at any time.

Regulatory Authorities

Jurisdiction	Regulator	Contact Details
United Kingdom	Information Commissioner's Office (ICO)	Website: https://www.ico.org.uk Address: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, UK
European Union (Lead Authority)	Data Protection Commission (Ireland)	Website: https://www.dataprotection.ie Address: 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland
Cayman Islands	Office of the Ombudsman	Website: https://ombudsman.ky Address: 2nd Floor, Anderson Square, 64 Shedden Road, George Town
Bermuda	Office of the Privacy Commissioner for Bermuda	Website: https://www.privacy.bm Address: Maxwellton House, 3rd Floor, 20 Parliament Street, Hamilton HM12
British Virgin Islands	Office of the Information Commissioner (BVI)	Website: https://gov.vg/ Address: 33 Admin Drive, Wickhams Cay 1, Tortola, British Virgin Islands
Hong Kong	Office of the Privacy Commissioner for Personal Data (PCPD)	Website: https://www.pcpd.org.hk Address: 17/F, Cambridge House, Taikoo Place, 979 King's Road, Quarry Bay
DIFC	Commissioner of Data Protection (DIFC)	Website: https://www.difc.ae/business/regulations/data-protection Address: Level 14, The Gate Building, DIFC, Dubai, UAE
ADGM	Office of Data Protection (ADGM)	Website: https://www.adgm.com/operating-in-adgm/office-of-data-protection Address: Al Maqam Tower, ADGM Square, Al Maryah Island, Abu Dhabi

17 UPDATES TO THIS PRIVACY STATEMENT



WPS may update or amend this Privacy Statement from time to time in order to reflect changes in applicable laws and regulations, developments in our business operations, or modifications to the way in which we process personal information.

Where such changes are made, the updated version of this Privacy Statement will be made available on our website. Where required by applicable Data Protection Laws, we will take appropriate steps to notify individuals of material changes, which may include providing additional notices or obtaining consent where necessary.

We encourage you to review this Privacy Statement periodically to ensure that you are aware of how your personal information is processed and protected.

18 CONTACT INFORMATION

18.1 Contact details

Any questions, requests or concerns in relation to this Privacy Statement, or regarding the processing of your personal information, should be directed to WPS using the contact details below:

Email: WPSLegal@walkersglobal.com

WPS has appointed a Data Protection Lead ("DP Lead") who is responsible for overseeing compliance with applicable Data Protection Laws and this Privacy Statement. The DP Lead can be contacted using the contact details set out above.

WPS will endeavour to respond to all queries and requests in accordance with applicable Data Protection Laws and within the timeframes prescribed by those laws. Where appropriate, WPS may request additional information to verify your identity before responding to any request.

18.2 Representative arrangements

- **UK Representative:** Walkers Professional Services (UK) Limited
- **EU Representative:** Walkers Corporate Services (Ireland) Limited
- **Lead Supervisory Authority:** Data Protection Commission (Ireland)

19.3 Entities and Contact Details

Jurisdiction	Entity	Address
Cayman Islands	Walkers Professional Services (Cayman) Limited	190 Elgin Avenue, George Town, Grand Cayman, KY1-9001, Cayman Islands
Ireland	Walkers Corporate Services (Ireland) Limited	The Exchange, George's Dock, IFSC, Dublin 1, D01 W3P9, Ireland
United Kingdom	Walkers Professional Services (UK) Limited	1 Blossom Yard, Fourth Floor, London, E1 6RS, United Kingdom
Bermuda	Walkers Corporate Services (Bermuda) Limited	Park Place, 55 Par La Ville Road, Ground Floor, Hamilton HM11, Bermuda
British Virgin Islands	Walkers Corporate Services (BVI) Limited	PO Box 92, 171 Main Street, Road Town, Tortola, VG1110, British Virgin Islands
Hong Kong	Walkers Corporate Services (Hong Kong) Limited	15th Floor, Alexandra House, 18 Chater Road, Hong Kong
DIFC (Dubai)	Walkers Professional Services (Middle East) Limited (or DIFC Entity)	Office 501, Suite 115, Floor 05, Tamouh Tower, Tamouh, Al Reem Island, Abu Dhabi, United Arab Emirates



ADGM (Abu Dhabi)	Walkers Professional Services (ADGM) Limited	ADGM Square, Al Maryah Island, Abu Dhabi, UAE
-------------------------	--	---

August 2026