

Privacy Notice

How we collect, use, share and protect personal data. Jersey and the United Arab Emirates.

VERSION 3.0, 4 SEPTEMBER 2026

FGC comprises three entities. This notice covers all of them. It explains what personal data we collect, why we use it, who we share it with, how long we keep it, and what rights you have.

Two data protection regimes apply to us. The Data Protection (Jersey) Law 2018 (the "DPJL") applies to our Jersey entities. United Arab Emirates Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (the "UAE PDPL") applies to our Ras Al Khaimah entity.

In this notice, "Data Protection Legislation" means the DPJL, the Data Protection Authority (Jersey) Law 2018, the UAE PDPL, and any other data protection law applicable to us.

"Controller", "data subject", "process" and "personal data" have the meanings given to them in the applicable law.

1. WHO WE ARE, AND WHICH OF US CONTROLS YOUR PERSONAL DATA

- 1.1 Rory Forrest owns and operates all three entities. Each is a separate controller of the personal data it processes. They are not joint controllers, and none of them is liable for the acts of another.

FGC Legal Services: the registered business name under which Rory Forrest, Advocate of the Royal Court of Jersey, practises. It provides legal services under Jersey law and is established in Jersey. The DPJL applies, and its supervisory authority is the Jersey Office of the Information Commissioner.

FGC Legal Consulting Ltd: registered in Jersey, number 160210. It provides consulting services: fractional in-house legal and governance capability, legal infrastructure, documents and playbooks. It is established in Jersey. The DPJL applies, and its supervisory authority is the Jersey Office of the Information Commissioner.

FGC Legal Consulting FZ-LLC: RAKEZ licence number 47033676. It provides consulting services, and legal consultancy on the laws of jurisdictions other than the United Arab Emirates. It is established in the Ras Al Khaimah Economic Zone, United Arab Emirates. The UAE PDPL applies, and its supervisory authority is the competent United Arab Emirates data protection authority.

- 1.2 Which entity controls your personal data depends on your relationship with us:
- (a) If you are a client, or work for one, the controller is the entity named in your engagement letter.
 - (b) If you have asked us for a proposal but have not yet engaged us, the controller is the entity that would provide the services, as identified in the proposal.
 - (c) If you are a director, shareholder, beneficial owner, officer or connected person of a client, the controller is the entity engaged by that client.
 - (d) If you are a counterparty, or an adviser to a counterparty, in a matter we are working on, the controller is the entity engaged on that matter.
 - (e) If you visit our website, subscribe to our writing, or contact us without a matter attached, the controller is FGC Legal Consulting Ltd.

- (f) If you apply to work with us, the controller is the entity you applied to.

- 1.3 If you are not sure which entity holds your personal data, ask us and we will tell you.

2. HOW TO CONTACT US

- 2.1 Write to us at rory@fgc.law, or to Rory Forrest, 3 Brookhill Farm, La Rue du Pre, St Saviour, Jersey JE2 7UH.
- 2.2 Use the same address for a request to exercise your rights, whichever entity holds your personal data.
- 2.3 We are not required to appoint a data protection officer under either law, and we have not appointed one. Rory Forrest is accountable for data protection across all three entities.

3. WHAT PERSONAL DATA WE COLLECT

We collect and process the following categories of personal data:

- (a) **Identity data:** name, date and place of birth, nationality, government-issued identification numbers, photographic identification, and signature.
- (b) **Contact data:** postal address, email address, and telephone numbers.
- (c) **Professional data:** job title, employer, company affiliations, directorships, shareholdings, professional qualifications, and regulatory status.
- (d) **Correspondence and matter data:** records of our communications with you, meeting and call notes, instructions, documents you give us, documents we produce, and the substance of the matter itself.
- (e) **Financial data:** bank account and payment details, billing address, invoices, and records of payment.
- (f) **Client due diligence data:** source of funds and source of wealth information, corporate structure and beneficial ownership information, screening results for sanctions, politically exposed persons and adverse media. It also includes the documents that support that information. This category is collected by FGC Legal Services, which carries on supervised business in Jersey, and by FGC Legal Consulting FZ-LLC where the United Arab Emirates anti-money laundering regime applies to the engagement.
- (g) **Matter management data:** time records, fee estimates, matter status and internal file notes.
- (h) **Technical data:** IP address, browser type and version, device information, operating system, time zone setting, and how you use our website. Our cookie policy, published on our website, explains the cookies we use.
- (i) **Marketing data:** your preferences about receiving our writing and updates, and whether you have opened or clicked on what we send.
- (j) **Anything else you give us** in the course of instructing us or corresponding with us.

4. SENSITIVE AND SPECIAL CATEGORY PERSONAL DATA

Some legal and consulting work involves personal data that the law treats as needing extra protection. The two regimes define this differently, so we set out each.

- 4.1 **Under the DPJL.** Special category data is personal data about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, and criminal record or alleged criminal activity. It also includes genetic and biometric data used to identify a person.
- 4.2 Where we process special category data, we rely on a condition in Schedule 2, Part 2 of the DPJL. Most often the condition is that the processing is necessary to establish, exercise or defend legal rights or claims, that it is necessary for reasons of substantial public interest provided for by law, or that you have given explicit consent.
- 4.3 **Under the UAE PDPL.** Sensitive Personal Data is data that directly or indirectly reveals a person's family, ethnic origin, political or philosophical opinions, religious beliefs, criminal record or biometric data. It also includes data about a person's health or their physical, psychological, mental, genetic or sexual condition. Where our Ras Al Khaimah entity processes such data, it relies on a case set out in Articles 4 and 6 of the UAE PDPL. Most often the case is that the processing is necessary to protect or exercise a legal right or to defend a claim, that it is necessary to perform a contract, or that you have consented.
- 4.4 In practice we encounter this data most often in client due diligence, where screening returns information about criminal proceedings or political exposure, and where a matter itself concerns a regulatory or criminal issue.

5. HOW WE COLLECT YOUR PERSONAL DATA

We obtain personal data in three ways.

- 5.1 **Directly from you,** when you ask us for a proposal, engage us, give us documents or instructions, complete our onboarding and client due diligence process, contact us by any means, complete a form on our website, subscribe to our writing, or apply to work with us.
- 5.2 **By generating it ourselves,** in the course of providing the services: our notes, our analysis, our advice, our time records, and the documents we draft.
- 5.3 **From third parties and public sources,** including your employer or the entity you act for, our client where you are a connected person of that client, and other advisers and lawyers working on the same matter. The public sources and specialist providers we use are companies registries and beneficial ownership registers, sanctions and politically exposed person lists, credit reference and identity verification providers, court and tribunal records, regulators, news media and professional networking sites.
- 5.4 Where the law requires us to tell you the source of personal data we did not obtain from you, we will do so on request.

6. WHY WE USE YOUR PERSONAL DATA, AND OUR LAWFUL BASIS

- 6.1 Each purpose below is followed by the basis on which each regime permits it. Our Jersey entities rely on the DPJL basis (Article 9 of, and Schedule 2 to, the DPJL).

Our Ras Al Khaimah entity relies on the UAE PDPL basis (Articles 4 and 6).

To assess a proposed engagement and decide whether to accept it, including conflict checks: DPJL: steps at your request with a view to entering a contract, and our legitimate interests. UAE PDPL: steps preparatory to a contract.

To provide the services described in the engagement letter: DPJL: performance of our contract with you. UAE PDPL: performance of a contract.

To communicate with you about a matter: DPJL: performance of our contract with you. UAE PDPL: performance of a contract.

To carry out client due diligence, screening and ongoing monitoring, where we are required by law to do so: DPJL: compliance with a legal obligation. UAE PDPL: compliance with a legal obligation.

To comply with our professional, regulatory and reporting obligations: DPJL: compliance with a legal obligation, and our legitimate interests. UAE PDPL: compliance with a legal obligation.

To invoice you and collect payment: DPJL: performance of our contract with you, and our legitimate interests. UAE PDPL: performance of a contract.

To manage our practice, including file management, supervision, risk management and insurance: DPJL: our legitimate interests. UAE PDPL: your consent, given by accepting our engagement terms.

To develop our know-how, precedents and templates, and to train our people: DPJL: our legitimate interests. UAE PDPL: your consent, given by accepting our engagement terms.

To use artificial intelligence tools in delivering the services, as section 7 explains: DPJL: performance of our contract with you, and our legitimate interests. UAE PDPL: performance of a contract.

To send you our writing and updates about our services: DPJL: your consent, or our legitimate interests where you are an existing client and have not objected. UAE PDPL: your consent.

To operate and secure our website and systems: DPJL: our legitimate interests. UAE PDPL: your consent, given by accepting our engagement terms.

To establish, exercise or defend legal rights and claims, including our own: DPJL: necessary for legal proceedings, obtaining legal advice, or establishing, exercising or defending legal rights. UAE PDPL: necessary to protect or exercise a legal right or defend a claim.

To consider a job or contractor application: DPJL: steps at your request with a view to entering a contract, and our legitimate interests. UAE PDPL: steps preparatory to a contract.

- 6.2 Where we rely on our legitimate interests under the DPJL, those interests are running a legal and consulting practice competently, managing our risk, meeting our professional obligations, and developing the quality of our work. We have satisfied ourselves in each case that doing so does not override your interests, rights and freedoms. Ask us if you would like to know more about that assessment.

- 6.3 The UAE PDPL works differently. Processing requires your consent unless one of the cases in Article 4 applies. Where we state consent as the UAE PDPL basis, our engagement terms record it.

- 6.4 Where we rely on your consent, you may withdraw it at any time. Withdrawing consent does not affect processing carried out before you withdrew it, and it

does not affect processing we carry out on another basis.

7. OUR USE OF ARTIFICIAL INTELLIGENCE

We use artificial intelligence tools, including large language models, in delivering our services. We use them for legal and factual research, drafting, document review and comparison, summarising, and the operational work of running a matter and running the practice.

7.1 **We use these tools on business terms, not consumer ones.** The tools we use are **Claude for Work** (Anthropic's commercial offering), **ChatGPT Business** (OpenAI's commercial offering), **Perplexity** (Perplexity AI's commercial offering), and **Microsoft 365 Copilot**. Each is subscribed on the provider's commercial or business terms, under which the provider does not use our inputs or outputs to train or improve its models. We do not use free or personal-subscription artificial intelligence services for client work, and we do not paste client material into publicly available tools. The Law Society of Jersey's guidance on artificial intelligence warns members against putting confidential or privileged client information into open or publicly available systems. Our arrangements are built with that warning in mind.

7.2 When we use these tools:

- (a) a person with the relevant professional judgement reviews every output before it goes to a client;
- (b) we remain fully responsible for the work, exactly as if no such tool had been used;
- (c) we use only providers that are contractually prohibited from using our clients' confidential information or personal data to train or improve their models;
- (d) we apply technical and contractual safeguards to protect confidentiality and, where the work is legal services, legal professional privilege; and
- (e) we do not use these tools to make a decision about any individual without human involvement.

7.3 A client may tell us in writing that they do not want us to use these tools on their matter, and we will respect that.

8. WHO WE SHARE YOUR PERSONAL DATA WITH

We share personal data with the following categories of recipient.

- (a) **Our technology providers**, who process personal data on our instructions under written contracts: providers of document management, email and productivity, practice and matter management, client due diligence and screening, artificial intelligence services, hosting of our research and know-how systems, accounting, and website and security services. Our Provider Privacy Schedule lists the providers we currently use, what each does for us, where each stores personal data, and where to find each provider's privacy information. We will give it to you on request.
- (b) **Other professional advisers and service providers on your matter**, including advocates and counsel, foreign lawyers, experts, notaries, accountants, tax advisers, corporate service providers, banks and agents, where they need the personal data to do their part of the work.
- (c) **Our own advisers and insurers**, including our accountants, our professional indemnity insurers and

brokers, and any lawyers we instruct for ourselves. They are bound to keep it confidential.

- (d) **Regulators, authorities and courts**, where the law requires or permits it or where it is necessary for legal proceedings. Which of them applies depends on the entity and the matter. FGC Legal Services is regulated by the Law Society of Jersey and supervised by the Jersey Financial Services Commission for anti-money laundering purposes. Recipients may also include the Jersey Financial Intelligence Unit, the United Arab Emirates Financial Intelligence Unit, tax authorities, and courts and tribunals.
- (e) **Companies registries and filing authorities**, where a matter requires a filing that includes personal data.
- (f) **A buyer or successor**, if we sell or reorganise our business, subject to appropriate confidentiality protections.

9. INTERNATIONAL TRANSFERS

Our work is cross-border. Personal data moves between our entities and to service providers in the United Kingdom, the European Economic Area, the United States and the United Arab Emirates.

9.1 We transfer personal data out of Jersey, or out of the United Arab Emirates, only where the law allows it. That means one of the following applies:

- (a) the destination is recognised as providing adequate protection for personal data, which covers the United Kingdom and, for a provider certified under the EU-US Data Privacy Framework, the United States;
- (b) appropriate safeguards are in place, most often the European Commission's standard contractual clauses incorporated in the provider's data processing terms; or
- (c) the transfer is necessary to perform a contract with you or to establish, exercise or defend legal claims, or you have consented to it.

9.2 Our three entities share common systems, hosted in the United Kingdom, the European Union and the United States. Each entity controls the personal data on its own matters within them. Where personal data passes from a Jersey entity to our United Arab Emirates entity, it does so for a specific matter and on one of the grounds above.

9.3 You may ask us for details of the safeguards applied to a particular transfer.

10. DATA SECURITY

10.1 We have technical and organisational measures in place to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage, as Article 21 of the DPJL and Article 20 of the UAE PDPL require.

10.2 Those measures include encryption of data in transit and at rest, multi-factor authentication on all business systems, access controls that limit access to those who need it, managed devices with disk encryption, backup and recovery arrangements, and contractual security obligations on our service providers. We review them regularly as threats change.

10.3 We are a cloud-based practice. No method of transmission over the internet and no method of electronic storage is entirely secure, and we cannot guarantee absolute security.

10.4 We have procedures for dealing with a personal data breach, and we will notify the relevant authority and

affected individuals where the law requires it. Article 20 of the DPJL and Article 9 of the UAE PDPL govern those obligations.

11. HOW LONG WE KEEP YOUR PERSONAL DATA

11.1 We keep personal data only as long as we need it for the purposes in this notice and to meet our legal, regulatory, professional and insurance obligations.

Legal services matter files: 11 years from the date the matter closes, as the Law Society of Jersey Code of Conduct requires. We keep a file longer only for a specific recorded reason, such as an open dispute or a beneficiary who is still a minor, and never beyond 20 years.

Original documents of intrinsic value, such as a will or a share certificate: until you instruct us otherwise. We do not destroy them.

Consulting services engagement files: the same 11-year period from the date the engagement closes. Both kinds of file are held in the same document management system, so we apply one rule to both.

Client due diligence records: at least five years from the end of the business relationship or the completion of the transaction, as Jersey and United Arab Emirates anti-money laundering laws require. In practice this sits inside the 11-year matter file period.

Email and message copies: matter correspondence is filed to the matter and kept with it for the matter file period. The copy left in our mailbox is a duplicate and is deleted on a rolling basis after three years.

Conversation histories in our artificial intelligence tools: not part of the matter record. Anything that matters is saved to the matter file. The histories themselves are deleted routinely.

Accounting and tax records: 10 years, as the Companies (Jersey) Law 1991 and the Income Tax (Jersey) Law 1961 require.

Declined engagements and unsuccessful proposals: two years from the date of the decision, so that our conflict records remain reliable.

Marketing data: until you unsubscribe or object, and then only a record that you have done so.

Job and contractor applications: 12 months from the decision, unless you agree to a longer period.

Website technical data: 13 months. The cookies we use, and how long each last, are set out in the cookie policy on our website.

11.2 We review our records for disposal once a year. At the end of the applicable period, we destroy or securely delete the personal data, unless we record a specific reason to keep it longer. Deleted data may remain in backups for a short period until those backups are overwritten.

12. MARKETING

12.1 We may send you our writing and updates about our services where you have subscribed, or where you are an existing client and we think they are relevant to you.

12.2 You can stop them at any time. Use the unsubscribe link in any email, or write to rory@fgc.law. We will act on your request promptly, and we will keep a record that you have unsubscribed so that we do not contact you again.

12.3 Article 17 of the UAE PDPL gives you a specific right to require us to stop processing your personal data for direct marketing, including profiling connected with it. Article 36 of the DPJL gives you an equivalent right.

12.4 We do not sell personal data, and we do not share it with third parties for their own marketing.

13. AUTOMATED DECISION-MAKING

13.1 We do not make decisions about you by wholly automated means, and we do not carry out profiling that produces legal effects for you or otherwise significantly affects you.

13.2 Some of our client due diligence screening is automated in the sense that a system generates a match against a sanctions, politically exposed person or adverse media list. A person always reviews the match and decides what to do about it. Article 38 of the DPJL and Article 18 of the UAE PDPL give you rights in relation to automated processing.

14. YOUR RIGHTS

Your rights depend on which law applies to the entity holding your personal data. Section 1 identifies that entity.

14.1 **Under the DPJL**, if the controller is FGC Legal Services or FGC Legal Consulting Ltd, you have the following rights:

- (a) **Access:** to be told whether we process your personal data, and to receive a copy of it together with information about how we process it.
- (b) **Rectification:** to have inaccurate personal data corrected and incomplete personal data completed.
- (c) **Erasure:** to have your personal data deleted where there is no longer a lawful reason for us to hold it.
- (d) **Restriction:** to have us limit our processing in certain circumstances, for example while we check whether data is accurate.
- (e) **Portability:** to receive personal data you gave us in a structured, commonly used and machine-readable format, and to have it transmitted to another controller, where the processing is based on consent or contract and is carried out by automated means.
- (f) **Objection:** to object to processing based on our legitimate interests, and to object at any time to processing for direct marketing.
- (g) **Automated decisions:** not to be subject to a decision based solely on automated processing that produces legal effects for you or otherwise significantly affects you.
- (h) **Withdrawal of consent:** where we rely on consent, to withdraw it at any time.

14.2 **Under the UAE PDPL**, if the controller is FGC Legal Consulting FZ-LLC, you have the following rights:

- (a) **To receive information:** to be given information about the personal data we process, the purposes, the recipients, and the safeguards applied to cross-border transfers.
- (b) **To request transfer:** to receive your personal data in a structured, machine-readable format and to have it transferred to another controller, where processing is based on consent or contract and is carried out by automated means.
- (c) **To correction or erasure:** to have inaccurate personal data corrected and to have your personal data erased, subject to our retention obligations.

- (d) **To restrict processing:** to have us limit our processing in certain cases.
 - (e) **To stop processing:** to require us to stop processing your personal data, including for direct marketing.
 - (f) **In relation to automated processing:** to object to a decision made by automated processing that has legal consequences for you.
 - (g) **Withdrawal of consent:** where we rely on consent, to withdraw it at any time.
- 14.3 **Limits that apply to all of these rights.** Some of these rights are qualified, and in a legal and consulting practice the qualifications matter:
- (a) We must keep certain records for a period the law fixes, so a request for erasure will not usually succeed against a matter file or a client due diligence record.
 - (b) Legal professional privilege and our duty of confidentiality to other clients may prevent us from disclosing material in response to an access request, including where the personal data of another person is mixed with yours.
 - (c) Where we are prohibited from telling you about a disclosure, such as a suspicion report, we cannot include it in a response.
 - (d) A right that depends on our relying on consent or contract does not apply where we rely on a different basis.
- We will always tell you if we cannot meet a request in full, and why.
- 14.4 **How to exercise a right.** Write to rory@fgc.law. We do not charge for a request. We may ask you to confirm your identity before we act, so that we do not disclose personal data to the wrong person. We will respond

within the period the applicable law allows, and we will tell you if we need longer and why.

15. THIRD-PARTY LINKS

Our website may link to other sites. We do not control them, and we are not responsible for their privacy practices. Read their privacy notices.

16. CHANGES TO THIS NOTICE

16.1 We may change this notice. The current version is always at www.fgc.law. Where a change materially affects how we process your personal data, we will tell you.

16.2 This notice was last updated on **4 September 2026**. It replaces all earlier versions, including the FractionGC privacy notice dated 15 September 2025.

17. COMPLAINTS

17.1 If you are unhappy with how we have handled your personal data, tell us first, at rory@fgc.law. We would rather put it right ourselves.

17.2 You may also complain to the supervisory authority at any time, whether or not you have raised it with us.

17.3 **If the controller is FGC Legal Services or FGC Legal Consulting Ltd**, complain to the Jersey Office of the Information Commissioner:

Jersey Office of the Information Commissioner, 2nd Floor, 5 Castle Street, St Helier, Jersey JE2 3BT.

Telephone: +44 (0) 1534 716530. Email: enquiries@jerseyoic.org. Website: jerseyoic.org.

17.4 **If the controller is FGC Legal Consulting FZ-LLC**, complain to the competent United Arab Emirates data protection authority, which is currently being reorganised. Contact us and we will tell you where to direct a complaint, and we will help you do it.