



PRIVACY NOTICE AND PRIVACY POLICY

FRA Privacy Notice

General

Forensic Risk Alliance (FRA) recognizes the importance of your privacy. This privacy notice is meant to inform you about the Personal Data we collect, use, share, or otherwise process in connection with your business relationship with FRA. If you have additional questions about FRA’s data collection practices after reading this notice, please contact us at privacy@forensicrisk.com.

This privacy notice is provided in a layered format so you can click through to the specific areas set out below. Please also use the Glossary at the end of this document to understand the meaning of some of the terms used in this privacy notice.

1. **[IMPORTANT INFORMATION AND WHO WE ARE](#)**
2. **[WHAT PERSONAL DATA WE COLLECT?](#)**
3. **[HOW DO WE COLLECT YOUR PERSONAL DATA?](#)**
4. **[FOR WHAT PURPOSES DO WE COLLECT, HOLD, AND USE YOUR PERSONAL DATA?](#)**
5. **[TO WHOM DO WE DISCLOSE YOUR PERSONAL DATA?](#)**
6. **[INTERNATIONAL TRANSFERS](#)**
7. **[INFORMATION SECURITY AND ACCURACY](#)**
8. **[HOW LONG WILL WE RETAIN YOUR INFORMATION?](#)**
9. **[YOUR RIGHTS IN RELATION TO YOUR PERSONAL DATA](#)**
10. **[GLOSSARY](#)**

I. Important Information and Who We Are.

Purpose of this Privacy Notice

This Privacy Notice explains how FRA collects, uses, shares and otherwise processes your Personal Data in connection with your relationship with us in accordance with applicable data privacy laws, including, without limitation, the General Data Protection Regulation (“GDPR”), which is in effect since 25 May 2018. We may provide supplemental privacy notices on specific occasions when we are collecting or processing Personal Data about you so that you are fully aware of how and why we are using your Personal Data.



Please note that this notice covers the processing that we carry out as a “data controller” of your Personal Data. FRA is made up of different legal entities which make up the FRA Group, details of which can be found here (<https://www.forensicrisk.com/legal/>). This privacy notice is issued on behalf of the FRA Group so when we mention "FRA", "we", "us" or "our" in this privacy notice, we are referring to the relevant company in the FRA Group responsible for processing your data. The EU representative of the FRA Group is Forensic Risk Alliance Limited. Forensic Risk Alliance, Inc. is responsible for this website.

FRA may process your Personal Data where we provide services to our clients. On certain client engagements, we are required to process your data on our client's behalf and per their instructions and, in such circumstances, we are acting as a “processor”. In such a situation, the data controller of your Personal Data is the company or other business entity which is our client and which instructs us to process your data in connection with using our services. This notice does not cover the processing of your personal data that we carry out as a "processor".

We have centralized all responsibilities for data protection matters at the FRA Group by appointing a global data privacy manager who is responsible for overseeing all questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your privacy rights, please contact us by email at privacy@forensicrisk.com. If you are based in the European Union (EU) you also have the right to make a complaint at any time to your national data protection supervisory authority. We would, however, appreciate the chance to deal with your concerns before you approach the regulator so please contact us in the first instance.

Personal Data

The term “Personal Data” as used in this privacy notice means any information relating to you from which you can be identified, such as your name, contact details, bank account details etc. Personal Data does not include data from which you can no longer be identified such as anonymized aggregate data.

2. What Personal Data Do We Collect?

We may collect different types of Personal Data about you which we have grouped together as follows: [Identity Data](#), [Contact Data](#), [Employment Data](#), [Financial Data](#), [Transaction Data](#), [Technical Data](#), [Usage Data](#) and [Marketing and Communications Data](#).

3. How Do We Collect Your Personal Data?

We use different methods to collect Personal Data from and about you including through:

- **Direct interactions.** You may give us your Identity and Contact Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes Personal Data you provide



when you visit our physical sites and locations; participate in an event we organize or at which we are present; or contact us (online or offline) or through our Contact Us form.

- **Automated technologies or interactions.** As you interact with our website, we may automatically collect Technical Data about your equipment, browsing actions and patterns. This may be collected through the use of cookies. For more information about our cookies please click <https://www.forensicrisk.com/cookies/>

- **Third parties or publicly available sources.** We may receive Personal Data about you from various third parties and public sources such as:
 - Technical Data from analytics providers; advertising networks; or search information providers;
 - Contact, Financial and Transaction Data from providers of technical, payment and delivery services.
 - Identity, Contact, and Employment Data from our clients, prospective clients and vendors.
 - Identity, Contact, Technical and Marketing and Communications Data from publicly available sources.

Where you use third-party social networking sites, the third-party social networking site controls the information it collects from you. For information about how they may use and disclose your information, including any information you make public, please consult their respective privacy policies. FRA is not responsible for the content or privacy practices of those other third-party websites.

4. For What Purposes Do We Collect, Hold, and Use Your Personal Data?

We collect Personal Data about you for various purposes including so that we can perform our business activities and functions, comply with our legal, regulatory and contractual obligations, and to provide our services to you.

Most commonly, we will use your Personal Data:

- To perform the contract we are about to enter into or have entered into with you or the company that you represent.
- For our legitimate interests (or those of a third party) and where your interests and fundamental rights do not override those interests, including to send you marketing information.
- To comply with a legal obligation.

Click [here](#) to find out more about the types of lawful bases that we will rely on to process your Personal Data.

We have set out below, in a table format, a description of the ways we plan to use your Personal Data, and, information on which of the legal bases we rely on to do so. Where we rely on legitimate interests as the legal basis, we have also identified what our legitimate interests are, where appropriate.

Purpose/Activity	Type of data	Legal basis
To respond to a request for information, request for proposal or other similar tender	(a) Identity (b) Contact (c) Financial (d) Transaction	Performance of a contract with you
To process your contract and deliver services (including register you as a client, manage payments, collections, fees and charges)	(a) Identity (b) Contact (c) Financial (d) Transaction	Performance of a contract with you (including client onboarding, project management, project performance and billing matters)
To manage our relationship with you which will include notifying you about changes to (a) our terms of use or (b) our privacy policy	(a) Identity (b) Contact (c) Marketing and Communications	(a) Performance of a contract with you (to inform you of any changes to our terms and conditions) (b) Necessary to comply with a legal obligation (to inform you of any changes to our privacy policy)
To provide information to potential investors in our business or potential buyers of the shares and/or assets of a member of the FRA Group, including in the in the context of a business reorganization or group restructuring exercise.	(a) Identity (b) Contact (c) Technical (d) Financial (e) Transaction	Necessary for the legitimate interests of a member of the FRA Group or a third party.
To administer and protect our business, our rights and/ or property (including collecting and recovery of money owed to us, this website, troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical (d) Financial (e) Transaction	Necessary for our legitimate interests (for running our business, providing administration and IT services, network security, to prevent fraud, and as may be required by law to comply with an order or legal process)
To improve our website, services, marketing, client relationships and experiences and to make suggestions and recommendations to you about services that may be of interest to you	(a) Contact (b) Identity (c) Technical (d) Usage (e) Marketing and Communications	Necessary for our legitimate interests (to define types of clients for our services, to keep our Website updated and relevant, to develop our business, to inform our marketing strategy, to develop our services and grow our business)
To process your application for a job opportunity with our company	(a) Identity (b) Contact (c) Employment	Necessary for our legitimate interests (to review your credentials and match them against the requirements of the position you have applied for)
To register you as a visitor to our offices and provide you access to our facilities	(a) Identity (b) Contact	Necessary for our legitimate interests



Please note that we may use or disclose Personal Data if we are required by law to do so or if we reasonably believe that use or disclosure is necessary to protect our rights and/or to comply with judicial or regulatory proceedings, a court order or other legal process.

What we may need from you

We may need to request specific information from you from time to time to help us confirm your identity and ensure your right to access Personal Data (or to exercise any of your other rights). This is another appropriate security measure to ensure that Personal Data is not disclosed to any person who has no right to receive it.

What if you do not provide the personal data we request?

It is in your sole discretion to provide Personal Data to us. If you do not provide us with all or some of the Personal Data we request, we may not be able, to provide all or some of our services, to enter into a contract with you or to send you company updates, industry news and invitations to our events.

Marketing and Business Development

We collect or generate information about you for the purposes of client relationship management, including marketing, business development and event management. Specifically information regarding email and/ or mailing preferences, event and meeting attendance, areas of business interest, records of correspondence with you and individuals connected to your business via post, telephone, email or online. Most information we collect about you comes from our direct interactions with you or publicly available information.

We may send you marketing communications if you have asked to receive such communications, if you are a client or if you are a business contact on the basis of legitimate interests and if you have not opted out of receiving that marketing.

We may share your Personal Data with third parties we work with for the purposes of hosting events.

We provide you with choices regarding certain Personal Data uses, particularly around marketing and advertising. You can view and make certain decisions about the use of your Personal Data at our [preference center](#).

You can ask us to stop sending you marketing messages at any time by unchecking relevant boxes to adjust your marketing preferences through our [preference center](#), by following the opt-out links on any marketing message sent to you, or by contacting us at any time by sending us an email at privacy@forensicrisk.com.

Where you opt out of receiving these marketing messages, this will not apply to Personal Data provided to us as a result of service purchase, service experience or other transactions.



5. To Whom Do We Disclose Your Personal Data?

We may share your Personal Data with the parties set out below for the purposes for which we will use your Personal Data as set out in Section 4.

- We may disclose your personal data to other members of the FRA Group, to the Boards of the members of the FRA Group, to third parties who are providing services to us, including IT service providers, event management, PR and marketing service providers, background and/or credit reference services, printers, telephone service providers and to document storage providers, backup and disaster recovery service providers.
- We may disclose your personal data to with law enforcement, legal and regulatory bodies and authorities, if we are under a duty to share your personal information in order to comply with any legal obligation; and/ or
- We may disclose your personal data to with third parties in the event that we sell any business or assets, including any shares of a member of the FRA Group, in which case we may disclose personal data we hold about you to the prospective and actual buyer of such business or assets.

6. International Transfers

We may have to transfer your Personal Data from the European Economic Area (EEA) to an FRA office or a third party outside of the European Economic Area. When we do we will always ensure that there is a legal basis and a relevant safeguard method for such data transfer so that your Personal Data is treated in a manner that is consistent with EU laws and other applicable laws and regulations on data protection. Measures include:

- Where required, FRA implements Standard Contractual Clauses approved by the EU Commission, or similar contractual clauses in other jurisdictions. This includes transfers to suppliers or other third parties. For further details, see [European Commission: Model contracts for the transfer of personal data to third countries](#)
- FRA has self-certified to the EU-US and Swiss-US Privacy Shield Frameworks, which programs require U.S. recipients of Personal Data from EU and Swiss residents to provide similar protection to Personal Data shared between the EU/Switzerland and the US. More information can be found below and on the EU Commission's website at [European Commission: EU-US Privacy Shield](#).

Please contact us at privacy@forensicrisk.com if you want further information on the specific mechanism used by us when transferring your Personal Data out of the EEA.



7. Information Security and Accuracy

We have implemented appropriate physical, administrative and technical safeguards to help us protect your Personal Data from unauthorized access, use and disclosure. We also require that our suppliers protect such information from unauthorized access, use and disclosure. We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

8. How Long Will We Retain Your Information?

We will only retain your Personal Data for as long as necessary to fulfil the purposes for which it was collected and processed, including for the purposes of satisfying any legal, regulatory, accounting or reporting requirements.

Upon expiration of the applicable retention period we will securely destroy your Personal Data in accordance with applicable laws and regulations.

We may retain your Personal Data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

9. Your Rights in Relation To Your Personal Data

You have rights you can exercise under certain circumstances in relation to your Personal Data that we hold, such as:

- Request access to your Personal Data.
- Request correction of your Personal Data.
- Request erasure of your Personal Data.
- Object to processing of your Personal Data.
- Request restriction of processing your Personal Data.
- Request transfer of your Personal Data.
- Right to withdraw consent.
- Request certain information regarding our disclosure of Personal Data to third parties for their direct marketing purposes.

You may have additional rights applicable to you under local law. If you wish to exercise any of the rights set out above, please contact us by email at privacy@forensicrisk.com



Changes to this Privacy Notice

We reserve the right to update this privacy notice at any time, and we will make an updated copy of such privacy notice available on our website.

The last revision date of revision will be updated so that you will always be able to understand what data we collect, how we use your data, and under what circumstances we may share your data with others.

It is important that the Personal Data we hold about you is accurate and current. Please keep us informed by sending us an email at privacy@forensicrisk.com if your Personal Data changes during your relationship with us.

10. GLOSSARY

Types of Personal Data:

- **Identity Data** may include first name and last name, gender and/or ethnicity
- **Contact Data** may include physical address, mailing address, email address, social media handle and telephone numbers
- **Employment Data** may include details of your employment history, i.e., profession, occupations, membership, skills or job titles, immigration information or travel history.
- **Financial Data** may include bank account or payment card details.
- **Transaction Data** may include details about payments to and from you and other details of services you have purchased from us.
- **Technical Data** may include internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access this website.
- **Usage Data** may include information about how you use our website and services.
- **Marketing and Communications Data** may include your preferences in receiving marketing from us and our third parties and your communication preferences

Lawful Basis:

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your Personal Data for our legitimate interests. We do not use your Personal Data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.



Performance of Contract means processing your information where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal obligation means processing your Personal Data where it is necessary for compliance with a legal obligation that we are subject to.

FRA Privacy Policy

EU-US and Swiss-US Privacy Shield

Forensic Risk Alliance complies with the EU-US and Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of Personal Information transferred from the European Union and Switzerland to the United States. Forensic Risk Alliance has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit:

<https://www.privacyshield.gov/>

In compliance with the Privacy Shield Principles, Forensic Risk Alliance commits to resolve complaints about our collection or use of your Personal Information. EU or Swiss individuals with inquiries or complaints regarding our Privacy Shield Policy should first contact Forensic Risk Alliance at:

Forensic Risk Alliance
c/o Privacy Complaints Department
Kacey Murphy/Gregory Mason
40 Westminster Street
Providence, RI 02903
USA
+1(401)-289-0866
privacy@forensicrisk.com

Forensic Risk Alliance has further committed to cooperate with EU data protection authorities (DPAs) with regard to unresolved Privacy Shield complaints concerning human resources data transferred from the EU in the context of the employment relationship. If you do not receive timely acknowledgment of your complaint from us, or if we have not addressed your complaint to your satisfaction, please contact the EU DPAs for more information or to file a complaint. The services of EU DPAs are provided at no cost to you.

Forensic Risk Alliance complies with the Privacy Shield Principles for all onward transfers of Personal Data from the EU and Switzerland, including the onward transfer liability provisions. Under certain conditions, more fully described on the Privacy Shield website at <https://www.privacyshield.gov>, you may invoke binding arbitration when other dispute resolution procedures have been exhausted.

Forensic Risk Alliance's participation in the Privacy Shield applies to Personal Data received from the EU/EEA and Switzerland. Forensic Risk Alliance will comply with the Privacy Shield Principles in respect of such



Personal Data. Some types of Personal Information may be subject to additional privacy-related requirements and policies, which are consistent with the Privacy Shield Principles.

Types of data Forensic Risk Alliance can potentially process generally falls into two categories.

1) Personal Information from Client Engagements: Forensic Risk Alliance provides professional consulting services to its clients. Forensic Risk Alliance's clients may send Personal Information to it for processing on their behalf as part of the consulting services they have purchased. For example, Forensic Risk Alliance may receive Personal Information such as name, email address, employment information or financial data. Forensic Risk Alliance uses any such Personal Information to perform services for its clients and to administer and manage its relationships with its clients. In the event that a client engagement involves a transfer of Personal Information from the EU or Switzerland to the United States, the relevant clients are responsible for providing appropriate notice, where required, to the individuals whose Personal Information may be transferred to Forensic Risk Alliance, including providing individuals with certain choices with respect to the use or disclosure of their Personal Information, and obtaining any requisite consent. Forensic Risk Alliance handles such Personal Information in accordance with its clients' instructions.

2) Personal Information regarding Forensic Risk Alliance Employees: Forensic Risk Alliance may transfer Personal Information regarding Forensic Risk Alliance personnel. This Personal Information may include, without limitation, business contact information, employee ID, job role and reporting line, demographic information, work history, compensation and performance ratings. Forensic Risk Alliance uses such information to administer and manage its business.

Choice and Accountability for Onward Transfer

Forensic Risk Alliance will not transfer, disclose, sell, distribute, or lease Personal Information to third parties other than as described in this Privacy Policy unless it has permission or is required or permitted by law (including to meet national security or law enforcement requirements). Forensic Risk Alliance may share such information with its affiliates as necessary to carry out the purposes for which the information was supplied, collected or received. Similarly, third party contractors, consultants and/or vendors engaged by Forensic Risk Alliance to assist it in providing its services may have access to such Personal Information (these third parties must first agree to maintain the strict confidentiality of such information and provide the same level of data security as provided by Forensic Risk Alliance). Forensic Risk Alliance remains responsible and liable under the Privacy Shield Principles if third-party agents that it engages to process the Personal Data on its behalf do so in a manner inconsistent with the Principles.

Information Security and Data Integrity

Forensic Risk Alliance is ISO 27001 certified has reasonable security policies and procedures in place to protect Personal Information from unauthorized loss, misuse, alteration, or destruction. Forensic Risk Alliance's ISO 27001 certification can be found here <https://www.forensicrisk.com/certification-iso27001/>. Despite Forensic Risk Alliance's best efforts, however, security cannot be absolutely guaranteed against all threats. To the best of Forensic Risk Alliance's ability, access to your Personal Information is limited to those who have a need to know.



Choice

When Forensic Risk Alliance collects Personal Information directly from custodians, we generally offer those custodians the opportunity to choose whether their Personal Information may be (i) disclosed to third party contractors, or (ii) used for a purpose that is materially different from the purposes for which the information was originally collected or subsequently authorized by the relevant custodian. To the extent required by the Privacy Shield Principles, Forensic Risk Alliance obtains opt-in consent for certain uses and disclosures of Sensitive Data. Consumers may contact Forensic Risk Alliance as indicated below regarding the company's use or disclosure of their Personal Information. Unless Forensic Risk Alliance offers custodians an appropriate choice, the company uses Personal Information only for purposes that are materially the same as those indicated in this Policy.

Forensic Risk Alliance shares Consumer Personal Information with its affiliates and subsidiaries. Forensic Risk Alliance may disclose Consumer Personal Information without offering an opportunity to opt out, and may be required to disclose the Personal Information, (i) to third-party Processors the company has retained to perform services on its behalf and pursuant to its instructions, (ii) if it is required to do so by law or legal process, or (iii) in response to lawful requests from public authorities, including to meet national security, public interest or law enforcement requirements. Forensic Risk Alliance also reserves the right to transfer Personal Information in the event of an audit or if the company sells or transfers all or a portion of its business or assets (including in the event of a merger, acquisition, joint venture, reorganization, dissolution or liquidation).

Access

If Forensic Risk Alliance holds your Personal Information, under most circumstances you have the right to reasonable access to that data to correct any inaccuracies. You can also make a request to update or remove information about you by contacting privacy@forensicrisk.com, and Forensic Risk Alliance will make all reasonable and practical efforts to comply with your request, so long as it is consistent with applicable law and professional standards.

Resource, Enforcement and Liability

Forensic Risk Alliance commits to resolve complaints about your privacy and its collection or use of your Personal Information in compliance with the EU-US and Swiss-US Privacy Shield Principles. Please contact Forensic Risk Alliance at: privacy@forensicrisk.com should you have a Privacy Shield-related (or general privacy-related) complaint.

If you are a resident of the EU/EEA or Switzerland, and you have a complaint related to this Policy that cannot be resolved with Forensic Risk Alliance directly, you may report your claim to the EU/EEA or Swiss Data Protection Authorities located in your jurisdiction. As further explained in the Privacy Shield Principles, a binding arbitration option will also be made available to you in order to address residual complaints not resolved by any other means.

Forensic Risk Alliance is subject to the investigatory and enforcement powers of the US Federal Trade Commission (FTC).



Questions and Comments

If you have questions or concerns regarding this Privacy Policy, related notices and how we process your information, please contact Forensic Risk Alliance at: privacy@forensicrisk.com. Forensic Risk Alliance may revise this Privacy Policy or any part of it at any time. Please review this Privacy Policy periodically for changes.

Last updated: October 2019