



UK APPLICANT PRIVACY NOTICE

Last updated: November 13, 2024

1. What does this notice cover?

This notice describes how Apex Fintech Solutions Inc. and its affiliates ("**Apex**", "**we**", "**us**" or "**our**") uses your personal data in connection with your application for employment with us. It also describes your data protection rights, including a right to object to some of the processing which Apex carries out. More information about your rights, and how to exercise them, is set out in the "Your choices and rights" section.

This notice applies to individuals who are located in the United Kingdom or European Economic Area that apply to, or enquire about, open employment opportunities at Apex. The data processing described in this notice may be limited as required by applicable law.

We also may provide you with additional information when we collect personal data, where we feel it would be helpful to provide relevant and timely information.

2. What categories of personal data we collect

- **Personal identification and communication information:** your name, any nickname or alias, video, audio, home address, phone number, email address, date of birth, gender, immigration status, and information about your entitlement to work;
- **Application-related information:** curriculum vitae (CV) or resume, cover letter, employment history, education history, qualifications and skills, reference contact information, position preferences, willingness to relocate, desired salary, interests and aspirations, background screening information if relevant and bank account information if we reimburse expenses;
- **Technical data:** online identifiers and IP address;
- **Virtual interview recordings:** digital recordings of virtual interviews which includes your voice, interview participation and may include your web camera footage;
- **Security information:** CCTV footage, access control system information, door entry system data and reception logs; and
- **Sensitive information:** for example, information about your health and disabilities where we need to make any reasonable adjustments; equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion, belief or community status.

We collect most of this information from you directly. For example, data is collected through our application portal and CVs; from correspondence with you; or through interviews, meetings or other assessments. We also collect some information about you from other people (e.g. recruitment agencies, referrals), your referees or organisations (e.g. from LinkedIn if you choose to connect us with your LinkedIn profile; where applicable, we also collect data from our third-party background screening provider during the pre-employment screening process).

3. Why we collect, use and store this personal data

We must have a legal basis to process your data. We explain each of these legal bases below. We also set out the purposes for which we process your data. For each purpose, we explain the lawful basis for that processing, the processing operations that we carry out and the categories of data that we process.

A. Legal basis

Consent – in certain limited cases, we ask for your consent to use your data. Whenever we ask with for your consent we will explain the situations where we use your data and for what purposes.

Legitimate interest – we can process your data when it is necessary for us to achieve a business purpose, or where it is necessary for someone else to achieve their purpose. We explain below what interests we, or others, are trying to achieve when we process your data. Where we process personal data on the basis of a legitimate interest, then – as required by data protection law – we have carried out a balancing test to document our interests, to consider what the impact of the processing will be on individuals and to determine whether individuals’ interests outweigh our interests in the processing taking place. You can obtain more information about this balancing test by using the contact details at the end of the notice.

Legal obligation – we have obligations to comply with legal and regulatory requirements under UK laws. In certain cases, we have to use your data to meet these obligations.

B. Purposes

We have set out below why we process your data and what data we use:

Processing your application – (legitimate interests)

We collect and use your personal data so we can process your application. We store, and where needed, update, your personal data to make informed decisions on recruitment and assess your suitability for the role, to communicate with you about your application, to respond to your inquiries and schedule interviews, and to reimburse you for any agreed expenses incurred in the application process.

To do this we use your personal identification and communication information. If we need to make adjustments for you during the recruitment process, we process special category data for this purpose.

This information will be shared with companies who host our recruitment portal and systems. If we reimburse expenses, we share information with financial service providers.

Processing your application – (consent)

With your consent, we will record your virtual interview(s) to help us make informed decisions on recruitment and assess your suitability for the role in cases such as if an interviewer is unable to attend.

To do this, we will use virtual interview recording information, including any data about you that this encompasses.

This information will only be share with companies who provide us with the services to record virtual meetings.

Keeping in touch – (consent)

With your consent, we use your data to contact you about future career opportunities at Apex. This includes storing your data, keeping it up to date and using it to contact you.



We use your personal identification and communication information and application-related information for this.

This information will be shared with companies who host our recruitment portal and systems.

Improving our recruitment process – (legitimate interests)

We have an interest in evaluating and improving our recruitment processes. To achieve this, we analyse your data, including identifying usage trends and comparing it to past recruitment processes.

We use your personal identification and communication information and application-related information for this purpose.

This information will be shared with companies who host our recruitment portal and systems.

Improving our recruitment process – (consent)

With your consent, we will record your virtual interview(s) for internal recruitment training purposes, such as for training employees how to conduct certain types of interviews, primarily technical software engineering assessments or behavioural interviews.

To do this, we will use a recording of your virtual interview, including any data about you that this encompasses.

This information will only be share with companies who provide us with the services to record virtual meetings.

Verifying information – (legitimate interests)

We have an interest in carrying out appropriate checks to verify the information provided by candidates. We verify the details you have supplied and, where applicable, conduct pre-employment background checks or if necessary, request proof of prior employment.

We use your personal identification information and communication related information, and application related information to do this.

This information will be shared with companies who host our recruitment portal and systems and with background screening companies. Where we check references or previous employment and education, we disclose the fact that you have applied to us to educational institutions and to previous employers.

Business interests – (legitimate interests)

We have an interest in protecting our business interests and legal rights, including, use in connection with legal claims, compliance, regulatory, auditing, investigative and disciplinary purposes and ethics and compliance reporting requirements.

This also includes protecting the security of our premises, employees, users, assets, systems, and intellectual property and enforcing company policies.

We also have an interest in analysing and monitoring the diversity of the workforce in accordance with applicable laws including, for example, compliance with equal opportunity employment laws.



To do this, we store, use and may transmit your personal identification and communication information, technical information, application-related information and sensitive information.

This information will be shared with companies who host our recruitment portal and systems. Information used for diversity monitoring will be shared with a specialist company that advises us on diversity. We share information with legal and other advisers if there are investigations or potential claims.

Compliance with law – (legal obligation)

We use your data to comply with legal, regulatory and other requirements under UK laws by analysing and possibly transmitting your personal data.

We assess your fitness and propriety in connection to your engagement in a controlled function, where applicable, by analysing your data. To do this we use your personal identification and communication information, and application-related information.

Additionally, we are subject to legal requirements to carry out equal opportunities & diversity monitoring of our applicants, including ensuring fair participation by members of the Protestant and Roman Catholic communities. We conduct equality and anti-discrimination-related processing to the extent required by applicable law, including the Fair Employment & Treatment (NI) Order 1998. To do this we use your personal identification and communication information, application-related information and sensitive information (community background).

This information will be shared with companies who host our recruitment portal and systems and with regulators of UK government bodies where required by law.

Compliance with US law – (legitimate interests)

We use your data to comply with legal, regulatory and other requirements under US laws by retaining copies of your communications with us.

Apex is subject to a variety of US legal and regulatory requirements that require us to process your personal data contained in your application and any written communications you have with us. These requirements come from US financial services regulators including the Securities Exchange Commission (“SEC”), Financial Industry Regulatory Authority (“FINRA”), Commodity Futures Trading Commission (“CFTC”) and other US regulatory bodies such as US state and federal authorities (“US Regulators”).

Under these regulations and requirements, we are required to collect and maintain records of all communications that relate to the business of Apex, which includes applications to our open roles and any communications with us about our business. We are required to maintain this information for minimum mandatory retention periods as set by our US Regulators.

This information may be shared with our US Regulators to the extent we are required to by applicable law.

4. More information about verification and background checks

For certain positions, it will be necessary for us to verify the details you have supplied (for example, in relation to your identity, employment history, academic qualification and professional credentials) and to conduct pre-employment background checks (for example, in



relation to previous criminal convictions or financial standing). The level of checks will depend on your role, in particular whether you will occupy a regulated role, and will be conducted at as late a stage as is practicable in the recruitment process and often only after you have been selected for the position.

For example, if you are applying to a role which involves having regular access to books and records relating to securities or monies, you will be required to submit fingerprints to FINRA (and their appointed service provider) for processing in order to perform this role under US securities laws.

If your application is successful, we will provide further information about the checks involved and will obtain any necessary consent prior to completing such checks.

5. How we share your personal data

Other Apex entities

Personal data may be shared with our affiliates, including our parent companies, any joint venture partners or other companies that we control or that are under common control with us for the purposes above.

Personal data will primarily be processed by employees in our Human Resources, IT Finance, and Facilities departments. This will include sharing your personal data with our parent company Apex Fintech Solutions Inc. in the US and relevant hiring managers at our affiliates.

Your personal data will be shared with companies providing services, such as technology services including hosting, maintenance, administration and analysis, as well as other agencies, under contract to Apex as part of the recruitment process. When we share your data with these companies, it is in accordance with each purpose under section 3.

In the event that an Apex business is sold or integrated with another business, your details may be disclosed to our advisers and any prospective purchaser's adviser and will be passed to the new owners of the business.

Regulatory bodies and law enforcement

Your personal data will also be shared with US Regulators, UK government authorities and/or law enforcement officials if mandated by law or if required for the protection of our legitimate interests in compliance with applicable laws.

Equality Commission for Northern Ireland

Personal data, including your community background status and/or religious beliefs may be shared with the Equality Commission for Northern Ireland where required by law.

6. Where we transfer your personal data

As a US headquartered organization, most of our IT systems and information listed in section 2 above is hosted in the US. It will primarily be processed by employees in the Human Resources, IT and Finance, and Facilities departments and by your line manager.

We transfer your personal data to the US under the UK International Data Transfer Agreement ("IDTA") framework. A copy of this mechanism can be obtained for your review on request by using the contact details below.

7. Your choices and rights

You have the right to **ask Apex for a copy** of your personal data; to **correct, delete** or **restrict** processing of your personal data; and to **obtain the personal data you provide in a structured, machine-readable format**. In addition, you can **object to the processing** of your personal data in some circumstances (in particular, where we don't have to process the data to meet a contractual or other legal requirement).

Where we have asked for your consent, you may **withdraw consent** at any time. If you ask to withdraw your consent to Apex processing your data, this will not affect any processing which has already taken place at that time. You have an absolute right to opt-out of direct marketing, or profiling we carry out for direct marketing, at any time. You can do this by following the instructions in electronic message communications, through our applicant portal user control settings (if you have an account) or by contacting us using the details set out below. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law. However, it may take up to ten (10) business days for us to process and implement your request.

These **rights may be limited**, for example if fulfilling your request would reveal personal data about another person, or if you ask us to delete information which we are required by law or have compelling legitimate interests to keep. If you have unresolved concerns, you have the **right to complain** to a data protection authority. In the UK, this will be the Information Commissioner.

Where we collect personal data to administer a contract with you or to comply with our legal obligations, this is mandatory and we will not be able to manage the application relationship without this information. In all other cases, provision of the requested personal data is optional, but this may affect your ability to participate in certain programs or systems, where the information is needed for those purposes.

Some or all of your rights may be exercisable by logging into our Careers website and accessing your profile settings. Your rights can otherwise be exercised by contacting us in Section 10 "Contact us" below.

8. How long we retain your personal data

If you are successful: we will retain your personal data only for as long as we need it for Apex's legitimate interest in accordance with applicable law, for the purposes of the recruitment process and, once this process is finished, for an appropriate period so as to be able to deal with any legal claims linked to the application process. Recruitment records for successful applicants are generally kept for 7 years. After this period, we will take steps to delete your personal data or hold it in a form that no longer identifies you. If you become an Apex employee, relevant personal data you provide will become a part of your employee file and may be used later for the management of the employment relationship.

If you are not successful: we will retain your personal data with your permission for 12 months or as long as we are required to by applicable laws.

9. Updates to this privacy notice

We reserve the right to update this privacy notice at any time. The latest version of this privacy notice will be posted on our website and if we have your contact information we will provide



you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

10. Contact us

The data controllers for your personal data will be:

Controller	When applicable
Apex Fintech Solutions UK Ltd	For all roles out of our Belfast office
PEAK6 Group LLC	For all roles (HR system admin)
Apex Clearing Corporation	For all roles supporting Apex Clearing Corporation
Apex Silver LLC	For all roles supporting Apex Silver
The Evil Geniuses (EG) LLC	For all roles supporting Evil Geniuses

If you have questions about this privacy notice or wish to contact us for any reason in relation to our personal data processing, please contact us at the following address:

Email: workforceprivacy@apexfintechsolutions.com