IMMERSIVELABS

Candidate Privacy Notice

Effective from November 2023 | Version 11.23

This privacy notice tells you how we look after your personal data when we process your personal data in as a prospective employee at Immersive Labs.

This privacy notice tells you what personal data Immersive Labs collects about you, what we use it for and who we share it with. It also explains your rights and what to do if you have any concerns.

This privacy notice will supplement any other notices you receive from us and they should be read together. We may need to make changes to this notice occasionally, to reflect any changes to our services or legal requirements. We will notify you of any important changes before they take effect. This notice was last updated on 17 November 2023.

1. WHO WE ARE AND OTHER IMPORTANT INFORMATION

We are Immersive Labs Group (**Immersive Labs, we, us** or **our**) which is formed of the following companies:

Immersive Labs Holdings Limited (registered in England and Wales under company number 11439032 with its registered office at Runway East, 1 Victoria Street, Bristol, BS1 6AA, England)

Immersive Labs Limited (registered in England and Wales under company number 10553244 with its registered office at Runway East, 1 Victoria Street, Bristol, BS1 6AA, England)

Immersive Labs Corporation (registered in Delaware, USA with its office at WeWork, 200 Berkeley St, Boston, 02116 MA, USA)

Immersive Labs GmbH (registered in Düsseldorf, Germany with its office at c/o RSM GmbH, Georg-Glock-Straße 4, 40474 Düsseldorf

Immersive Labs Cyber Security Services LLC (registered in United Arab Emirates with its office at Emirates Towers Office Tower, Trade Center Second, Sheikh Zayed Road, Dubai, United Arab Emirates)

As a prospective employer, Immersive Labs will be 'controller' of your information, which means that it decides what personal data we collect from you and how it is used. Immersive Labs Ltd is registered with the Information Commissioner's Office, the UK regulator for data protection matters under number ZA281110.

We process personal data in accordance with our obligations under the GDPR, the UK GDPR, the UK Data Protection Act 2018, the BDSG, the PDPL and all other applicable national, federal, state, provincial, and local laws and regulations governing the use and disclosure of personal information in the countries in which we process personal data.

Immersive Labs Corporation complies with the EU-U.S. Data Privacy Framework (**EU-U.S. DPF**) and the UK Extension to the EU-U.S. DPF, as set forth by the U.S. Department of Commerce. Immersive Labs Corporation has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (**EU-U.S. DPF Principles**) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. If there is any conflict between the terms in this privacy notice and the EU-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (**DPF**) Program, and to view our certification, please visit https://www.dataprivacyframework.gov/. For more information about Immersive Labs' participation in the EU-US Data Privacy Framework, please see Section 8 (Data Privacy Framework).

CONTACT DETAILS

Email address: legal@immersivelabs.com
Postal address: Immersive Labs, 6th Floor, the Programme, All Saints' St, Bristol, England, BS1 2LZ.

KEEPING US UPDATED

We want to make sure that your personal data is accurate and up to date. Please let us know about any changes so that we can update our systems for you.

2. THE PERSONAL DATA WE COLLECT ABOUT YOU

Personal data means any information which does or could be used to identify a living person. We collect the following types of personal data:

Personal Data Category	Example of Personal Data
Identifiers	Contact details, such as full name, alias, home address, phone number, email address (work and personal), IP Address, national insurance number, social security number, pronouns and date of birth.
Diversity and Inclusion Information	Including religion and spiritual beliefs, race, ethnicity, family status, health data including disability, veteran status, sexual orientation, sex and gender identification.
Professional and employment-related information	Job title, details of your qualifications, skills, experience and employment history, including start and end dates with previous employers and references, location of employment or workplaces, online application forms or CVs, notes and recordings from interviews and short-listing exercises.
Right to Work	Information about your nationality and entitlement to work in the country you are located.
Health Information	Information about your health, including any medical condition for which we need to make reasonable adjustments.

Identity Documentation	Passport, driving licence or equivalent.
Criminal and Credit Related Information	Criminal conviction history data, motor vehicle records and credit history.
Chat and Video Messaging	Meeting video recordings.

Aggregated and anonymous Data

When we collect personal data, we sometimes anonymise it (so it can no longer identify you as an individual) and then combine it with other anonymous information to form 'Aggregated Data'. Data Protection Legislation does not restrict us when it comes to how we use Aggregated and Anonymous Data and the various rights described below do not apply to Aggregated or Anonymous Data.

Special category personal data

Some of the personal data we collect is referred to as "**Special Category Personal Data**" because it is particularly sensitive and requires additional protections. We collect the following types of Special Category Personal Data:

- Information about your health, including any medical condition, if you choose to provide it, so that we can make any necessary reasonable adjustments as required by law.
- Equal opportunities monitoring information, including information about your gender, sexual orientation, ethnic origin, family status and health. We collect this personal data for the purposes set out below.

Equal opportunities monitoring

Where Immersive Labs processes personal data for the purposes of equal opportunities monitoring, such as information about your gender, ethnic origin, sexual orientation, health, and family status, it is considered Special Category Personal Data. We collect this type of information to help us eliminate inequality in hiring based on potential bias. We only collect this information where we have your consent and there will be no consequences (either positive or negative) of choosing to provide that consent or not. if you do give your consent, you can withdraw it at any time.

We will use the data we collect for internal equal opportunities monitoring to help us ensure we're attracting and retaining a diverse workforce, identify and eliminate any bias in our recruitment processes and identify barriers to workforce equity and diversity.

Criminal record data

We process personal data relating to criminal offences, which is also considered sensitive data under the data protection legislation.

We always collect criminal offence data relating to all employees, workers and contractors in the US and Canada as part of the pre-employment process.

We collect criminal offence data relating to employees in the UK and the rest of Europe as appropriate given the nature of the role and where we are legally able do so.

We only carry out criminal record checks upon a conditional offer of employment and we always ensure that we follow any applicable local legislation. We have in place an appropriate policy and safeguards which we may be required by law to maintain when processing such data.

3. HOW YOUR PERSONAL DATA IS COLLECTED

- **Direct interactions:** You provide your personal data to us by filling in forms or by corresponding with us by post, phone or email when you:
    - submit an application form or send us your cv
    - send us your passport or other identity documents such as your driving license
    - complete forms during the pre-employment process (such as equal opportunities monitoring questionnaires)
    - attend interviews or complete an assessment
- **Information provided by others.** We may receive personal data about you from:
    - recruitment agencies that may help us to identify potential prospective employees
    - professional networking service providers, such as Linkedin and Github
    - former employers for the purposes of verifying your employment history
    - third party background check providers, credit reference agencies and consumer reporting agencies, acting as our processors (which means they can only use your personal data in line with our instructions).

4. HOW WE USE YOUR PERSONAL DATA

The following table sets out why we process your personal data and our lawful basis for processing your personal data. We may rely on more than one lawful basis for processing your personal data depending on the context of the activity.

Purpose	Categories of Personal Data	Lawful Basis for Processing	Third Party Recipients
To process an application or facilitate an interview: When you apply for a role via Linkedin, through a recruitment agency or direct, we will process information to assess your suitability for a role and conduct interviews.	Identifiers, Financial Information, Benefits Information (related to current benefit entitlements only) and Professional and Employment-related information.	This processing is in the legitimate interests of Immersive Labs.	• Linkedin • Recruitment Agencies • Ashby ATS
To make any necessary reasonable adjustments: We will process health and medical related data to ensure we have appropriate measures in place to manage any reasonable adjustments you may need.	Identifiers, Health and Medical	This processing is necessary for compliance with a legal obligation to which Immersive Labs is subject to.	• Ashby ATS

To ensure a fair and equitable processes for prospective employees: When you apply for a role, we ask for your consent for us to process certain personal data for equal opportunities monitoring.	Diversity and Inclusion Information.	This processing is carried out on the basis of your consent. Providing this personal data is optional.	• Ashby ATS
To carry out criminal background checks: As a condition of employment in the USA and Canada, all prospective employees must undergo background checks. Some employees in the UK and EU, may undergo background checks depending upon their roles and responsibilities.	Identifiers, Criminal and Credit Related Information.	This processing is necessary for compliance with a legal obligation to which Immersive Labs is subject to.	• Checkr • DBS • Credence
To complete your right to work checks: Your personal data will be processed when we check your documentation to assess your right to work in the country in which you are being employed.	Identity Documentation.	This processing is necessary for compliance with a legal obligation to which Immersive Labs is subject to.	• ADP • Credence • Checkr

5. CHANGE OF PURPOSE

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the lawful basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

6. WHO WE SHARE YOUR PERSONAL DATA WITH

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the country in which you are located. If we do, you can expect a similar degree of protection in respect of your personal information.

Your information may also be shared internally, including with members of the people team, legal and finance teams, your hiring manager, and IT staff, if access to the data is necessary for performance of their roles and where required by law.

Third-party service providers include those suppliers (including contractors and designated agents) and other entities within our group.

We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

In certain unique situations, the need may arise for us to disclose your data to third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If such a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy notice.

7. INTERNATIONAL TRANSFERS

Some of your personal data may be processed outside of the EEA, or the country in which you are located. In such instances Immersive Labs will ensure that your data is only processed in such countries which have adequate protection for the rights and freedoms of your personal data or where there is an approved transfer mechanism in place between us (such as the Standard Contractual Clauses). We will always ensure that we have an appropriate written contract in place with our third party service providers which ensures the third party has adequate technical and organizational security measures in place to protect your data.

8. US DATA PRIVACY FRAMEWORK AND THE UK EXTENSION

Immersive Labs Corporation participates in the US Data Privacy Framework and the UK Extension to the US Data Privacy Framework set forth by the U.S Department of Commerce (hereinafter referred to as the "**DPF**").

Immersive Labs has certified to the U.S Department of Commerce that it adheres to the Principles laid down by the DPF with regard to the processing of personal data received from the EU and the UK. If there is any conflict between the terms in this privacy notice and the DPF Principles, the Principles shall govern. To learn more about the DPF program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

This Section 8 describes how Immersive Labs implements the DPF Principles for the personal data it processes on behalf of its customers and users.

1. **Notice** – this privacy notice sets out:
    a. the personal data we collect and the identity of our US entity (Immersive Labs Corporation) adhering to the DPF Principles;
    b. the purposes for which we collect and use personal data;
    c. how to contact us with any inquiries or complaints (in the US, EU and UK);
    d. the categories of third parties to which we disclose personal data, and the reasons we do so;
    e. the right for you to access your personal data; and
    f. the other rights you have in relation to your personal data that enable you to limit our use and disclosure of it.

2. **Dispute Resolution -** In compliance with the DPF, Immersive Labs commits to resolve DPF Principles-related complaints about our collection and use of your personal data. Individuals with inquiries or complaints regarding our handling of personal data received in reliance on the DPF should first contact us at privacy@immersivelabs.com. If we cannot resolve your complaint through our internal processes, we will cooperate and comply respectively with the advice of the panel established by the EU data protection authorities and the UK Information Commissioner's Office (ICO) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF in the context of the employment relationship.

3. **Binding Arbitration –** Individuals have the possibility, under certain conditions, to invoke binding arbitration for complaints regarding DPF compliance not resolved by the dispute resolution mechanism listed above. For additional information, please visit https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf?tabset-35584=2.

4. **Enforcement and Investigatory Powers of the FTC -** The Federal Trade Commission has jurisdiction over Immersive Labs' compliance with the DPF.

5. **Liability in Cases of Onward Transfers** - With respect to transfers of Personal Data to third-party Processors, Immersive Labs (i) enters into a contract with each relevant Processor, (ii) transfers Personal Data to each Processor only for limited and specified purposes, (iii) ascertains that the Processor is obligated to provide the Personal Data with at least the same level of privacy protection as is required by the DPF Principles, (iv) takes reasonable and appropriate steps to ensure that the Processor effectively processes the Personal Data in a manner consistent with Immersive Labs' obligations under the DPF Principles, (v) requires the Processor to notify Immersive Labs if the Processor determines that it can no longer meet its obligation to provide the same level of protection as is required by the DPF Principles, (vi) upon notice, including under (v) above, takes reasonable and appropriate steps to stop and remediate unauthorized processing of the Personal Data by the Processor, and (vii) provides a summary or copy of the relevant data protection provisions of the Processor contract to the Department of Commerce, upon request. Immersive Labs remains liable under the DPF Principles if Immersive Labs' third-party Processor onward transfer recipients process relevant Personal Data in a manner inconsistent with the DPF Principles, unless Immersive Labs proves that it is not responsible for the event giving rise to the damage.

9. HOW WE KEEP YOUR PERSONAL DATA SECURE

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed.

In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know it. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

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.

10. HOW LONG WE WILL KEEP YOUR PERSONAL DATA FOR

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the volume, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we use your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

For a list of all retention periods please email legal@immersivelabs.com.

In some circumstances you can ask us to delete your data: please see section 10 (your legal rights) for further information.

11. YOUR RIGHTS

You have specific rights when it comes to your personal data:

Access: You must be told if your personal data is being used and you can ask for a copy of your personal data as well as information about how we are using it to make sure we are abiding by the law

Correction: You can ask us to correct your personal data if it is inaccurate or incomplete. We might need to verify the new information before we make any changes.

Deletion: You can ask us to delete or remove your personal data if there is no good reason for us to continuing holding it or if you have asked us to stop using it (see below). If we think there is a good reason to keep the information you have asked us to delete (e.g. to comply with regulatory requirements), we will let you know and explain our decision.

Restriction: You can ask us to restrict how we use your personal data and temporarily limit the way we use it (e.g. whilst you check that the personal data we hold for you is correct)

Objection: You can object to us using your personal data if you want us to stop using it. We always comply with your request if you ask us to stop sending you marketing communications but in other cases, we decide whether we will continue. If we think there is a good reason for us to keep using the information, we will let you know and explain our decision.

Portability: You can ask us to send you or another organisation an electronic copy of your personal data

Complaints: If you are unhappy with the way we collect and use your personal data, you can complain to the UK Information Commissioner's Office but we hope we can help in the first instance. If you have any concerns you can email us at support@immersivelabs.co.uk.

Please note: not all of the above rights are absolute. There may be occasions whereby we cannot carry out your request however, we will always provide an explanation where this is the case.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is unfounded, repetitive or excessive.

All requests will be dealt with wherever possible within one month of receipt.

If you are a resident within the UK, you have the right to make a complaint at any time to the **Information Commissioner's Office (ICO),** the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO, so please contact us in the first instance.

If you are resident in another location, you can make a complaint to the applicable supervisory authority under the relevant local laws.

What we may need from you

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

We may also contact you to ask you for further information in relation to your request to speed up our response.

If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact us on legal@immersivelabs.com.

This privacy notice was updated in November 2023. For previous versions, please email legal@immersivelabs.com.