

End Users

End User Privacy Notice

www.immersivelabs.com



This privacy notice tells you what personal data Immersive 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.

1. Who We Are and Other Important Information

We are the Immersive Group (Immersive, 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 6th Floor, The Programme, All Saints' St, Bristol, England, BS1 2LZ)



Immersive Labs Limited (registered in England and Wales under company number 10553244 with its registered office at 6th Floor, The Programme, All Saints' St, Bristol, England, BS1 2LZ)



Immersive Labs Corporation (registered in Delaware, USA with its office at 501 Boylston 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)



In relation to our Website, Immersive will be the ‘controller’ of your information. Immersive will also be the ‘controller’ when you access the Platform in your capacity as an individual, and when we send marketing communications or otherwise use your personal data for security monitoring or analytics purposes. This means that we decide 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 (including but not limited to the CCPA and PIPEDA).

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’s participation in the EU-US Data Privacy Framework, please see Section 8 (Data Privacy Framework).

Where you are employed or engaged by our customer and are given access to our Platform by them, we will process some of your personal data on their behalf. In this case, they will be the ‘controller’ and we will be their ‘processor’.

Contact Details

Email address: legal@immersivelabs.com

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.

Third-Party Links

Our Website and Platform include links to external websites, plug-ins and applications provided by other organisations. By clicking on those links or enabling connections you may allow those organisations to collect or share personal data about you. We do not control how these organisations use your personal data, so we encourage you to read their privacy notices.

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 have grouped together the types of personal data that we collect below:



Identity Data - name and username



Contact Data - billing address, delivery address, job title, business email address, personal email address or academic email address and telephone numbers



Transaction Data - details of products and services we have provided to you and bank details (we do not process payment card details)



Technical Data - 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 on the devices you use to access our Website or Platform, SAML ID (when you access the Platform via SSO)



Profile Data - your username and password, your profile display photo, your job title or role, your interests, preferences, feedback and survey responses



Usage Data - information about your visit including the full Uniform Resource Locators (URL) clickstream to, through and from our site, reports, information you viewed or searched on our Website, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks and mouse-overs, lab completion activity and methods used to browse away from the page)



Marketing and Communications Data - your preferences in receiving marketing from us and our third parties and your communication preferences

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. This helps us identify trends (for example, what percentage of users access a specific product feature). Data protection law does not restrict us when it comes to how we use Aggregated Data and the various rights described below do not apply to Aggregated Data.

We do not intentionally collect any Special Categories of Personal Data (sensitive types of information which require additional protections, such as health information). However, we acknowledge that some information we collect could suggest special category data (for example, a user affiliated with a health charity or organisation could be inferred to have that health issue). You may also provide special category data to us voluntarily when you agree to take part in a case study, or when you otherwise communicate with us. We have controls in place to protect this information and we will only use it where we have a lawful basis for doing so.

3. How Your Personal Data Is Collected

- Direct interactions: You provide your personal data to us by filling in forms on the Website or by corresponding with us by phone or email when you:
 - apply for our products or services
 - create an account on our platform
 - submit requests for support
 - subscribe to our service or publications
 - allow us to send you marketing
 - enter a competition, prize draw, promotion or survey
 - give us some feedback or provide a case study
- Automated technologies or interactions: As you interact with our Website or Platform, we automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. Some cookies are not essential for us to provide our Website and Platform but enabling them will allow for a smoother and more tailored experience. For information about our use of cookies, please read our cookie policy.
- Information provided by others. We may receive personal data about you from:
 - technical service providers, acting as our processors (which means they can only use your personal data in line with our instructions)
 - marketing agencies and B2B databases that help us identify prospective customers
 - organisations such as your employer, if they are a customer of Immersive, and our partners, through which you may be given access to our Platform
 - organisations such as your prospective employer, if they are a customer of Immersive, and ask you to complete labs on the Platform as part of your assessment for a job-role.

4. How We Use Your Personal Data

We are required to identify a legal basis for collecting and using your personal data. There are six legal grounds on which organisations can rely on. The most relevant of these to us are where we use your personal data:

- to enter into and perform our contract with you (but only where the contract is with you as an individual, not a contract with another organisation)
- to comply with a legal obligation that we have
- to pursue our legitimate interests (our justifiable business aims) but only if those interests are not outweighed by your other rights and freedoms (for example, your right to privacy)
- to do something that you have given your consent for

This table sets out the legal ground that we rely on when we use your personal data for different purposes:

Purpose	Categories of personal data	Legal ground
Taking steps to enter into the contract with our customer (including any renewals) and general customer account management	Identity Data Contact Data	Performance of a contract (where our customer is an individual) Legitimate interests (where our customer is an organisation, as necessary to conclude our contract with the organisation and obtain contact details for key contracts)
Processing payments and collecting and recovering monies owed to us	Identity Data Contact Data Transaction Data	Performance of a contract (where our customer is an individual) Legitimate interests (where our customer is an organisation, as necessary to recover debts due to us)

Customer success administration	Identity Data Contact Data Profile Data Usage Data Transaction Data	Legitimate interests (where our customer is an organisation, as necessary to perform our contractual obligations to provide general customer support)
Professional services administration	Identity Data Contact Data Transaction Data	Legitimate interests (where our customer is an organisation, as necessary to perform our contractual obligations)
Handling requests for technical support	Identity Data Contact Data	Performance of a contract (where our customer is an individual) Legitimate interests (where our customer is an organisation, as necessary to perform our contractual obligations to provide technical support)
Providing access to our products, services and systems	Identity Data Contact Data Profile Data Usage Data Marketing and Communications Data	Performance of a contract (where our customer is an individual) Legitimate interests (where our customer is an organisation, as necessary to perform our contractual obligations to provide access to our products, services and systems)

Protecting our products, services and systems (and those of our processors)	Identity Data Technical Data Usage Data	Legitimate interests (necessary to monitor and improve network security and prevent fraud)
Providing insights into how our products and services are being used	Identity Data Contact Data Technical Data Profile Data Usage Data	Performance of contract (where our customer is an individual) Legitimate interests (where our customer is an organisation, to provide an overview of their users' engagement with the service)
Sending you service emails to notify you of objectives that have been assigned to you or that new content has been published	Identity Data Contact Data Technical Data	Legitimate interests (to effectively provide our products and services)
Sending you marketing communications by email	Identity Data Contact Data Technical Data Marketing and Communications Data	Consent (where you are a private individual, sole trader or partner in a partnership) Legitimate interests (where your email address belongs to an organisation which is a corporate body)

Asking you to participate in surveys and other types of feedback including (but not limited to) user research	Identity Data Contact Data Transaction Data Technical Data Profile Data Usage Data	Legitimate interests (necessary for product and service improvement purposes)
Asking you to participate in case studies	Identity Data Contact Data Transaction Data	Consent
Asking you to complete labs as part of an assessment for a job with a third-party organisation	Identity Data Contact Data Technical Data Profile Data Usage Data	Legitimate interests (necessary to provide our products and services).
Asking you to participate in a prize draw or competition	Identity Data Contact Data Technical Data Usage Data	Legitimate interests (necessary to provide the prize draw or competition and deliver a prize to you (if applicable)).
Notifying you about changes to our privacy notice	Identity Data Contact Data Profile Data	Legal obligation (necessary to comply with our obligations under data protection legislation)

If we plan to use personal data for a new purpose not listed in the table above, we will let you know beforehand and explain what legal ground we intend to rely on by updating this privacy notice and publishing it on our Website.

5. Marketing, Feedback and Research

If you access the platform in your capacity as an individual, we will get your consent before we direct marketing to you. This may include soft opt-in when we market similar products and services to you to the ones you have registered for.

If you access the platform in your capacity as an employee for your employer's organisation, we will send direct marketing to you unless you opt-out using the unsubscribe links in the footers of our emails. We do this because data protection legislation allows us to send directing market to corporate subscribers (e.g., business email addresses) under the lawful basis of legitimate interests (please see the table at Section 4 above).

Our direct marketing communications will always include a link so you can unsubscribe at any time, alternatively, you can withdraw your consent anytime by contacting us at legal@immersivelabs.com.

We sometimes use your information to form a view on what products, services or offers we think you might be interested in.

We may contact you if your recent activity suggests you might want to hear from us (for example, you entered one of our prize draws or competitions), unless you have already let us know you do not wish to receive marketing communications.

We may contact you to ask you to provide a case study about your experience on the Platform so that we can share your experience on our social media, website, and other promotional and marketing materials. We will always ask for your consent before we collect your information, and we will seek your approval of the final copy before your case study is published. You can withdraw your consent at any time by contacting us.

We may also get in touch with you to ask you to give us feedback or participate in user research so that we can improve our products and services. Where possible, we will remove identifiable personal data so that the feedback or research does not identify you as an individual. For example, for user research, we will remove your name (and any other identifiable information) from the data completely, and we will use pseudonyms when presenting the research internally.

If you participate in user research, we may ask you if we can record your voice and browser for the purposes of the exercise. For some types of research, we will also ask if we can record your video through your webcam, but this is less frequent. We use a third-party software provider to facilitate the research. We will always let you know before we access your camera, microphone and / or browser.

Please be aware that the software records your entire browser. Therefore, if you access other content on your browser outside the Immersive platform during your participation in the research, we may have access to such recorded content. As always, you can exercise any of your rights (under Section 12 below) in relation to this data.

6. Who We Share Your Personal Data With

- Our staff (our employees or other workers bound by contracts containing strict confidentiality and data protection obligations) – some of our staff may work for one of our group companies
- Our technical service providers including hosting, customer support, marketing and customer relationship, software monitoring, project management and customer insight providers (these organisations only have access to information they need to provide their services to us and are bound by contracts containing strict confidentiality and data protection obligations)
- Strategic partners such as resellers (businesses that sell Immersive products on our behalf). Strategic partners may have access to your organisation's account and will be able to set objectives on the Platform and view: (i) user profiles; (ii) complete and incomplete labs; and (iii) leader boards

- Customers (your employer or prospective employer) to give them information about your activity on the Platform, as necessary to provide our Services.
- Jobs partners where you apply for a job with one of our partners via our Cyber Million platform.
- Regulatory authorities such as HM Revenue & Customs, the UK tax authority
- Our professional advisers such as the accountants or legal advisors we sometimes use to help us conduct our business
- Any actual or potential buyer of our business

If Immersive is asked to provide personal data in response to a court order or legal request (e.g. from the police), we would seek legal advice before disclosing any information and carefully consider the impact on your rights when providing a response.

For a list of our Processors (defined below), please contact us at legal@immersivelabs.com.

7. Where Your Personal Data Is Stored

When we instruct organisations to process personal data on our behalf (our Processors) and that results in your information being sent outside of the UK or European Economic Area (EEA), we make sure that your information receives a similar level of protection by:

- only sending information to countries that have been formally recognised by the European Commission or the UK Government as having an adequate level of protection for personal data (including but not limited to organisations in the USA that participate in the Data Privacy Framework and the UK Extension to it); or
- using contracts approved by the European Commission and/or the UK Government to ensure appropriate safeguards are in place

If you are using our Platform because you have been enrolled by an organisation (e.g. your employer) then your personal data may be stored on servers located in the same region that they are based.

You can ask us for more information if you have a question about the information we send outside the UK or EEA.

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 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 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 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).

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's compliance with the DPF.
5. **Liability in Cases of Onward Transfers** - With respect to transfers of Personal Data to third-party Processors, Immersive (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's obligations under the DPF Principles, (v) requires the Processor to notify Immersive 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 remains liable under the DPF Principles if Immersive's third-party Processor onward transfer recipients process relevant

Personal Data in a manner inconsistent with the DPF Principles, unless Immersive proves that it is not responsible for the event giving rise to the damage.

9. Third-Party Marketing

We will get your consent before we share your personal data with any organisation outside Immersive for marketing purposes.

10. Cookies

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly.

For more information about the cookies we use, please see our [Cookie Policy](#).

11. How We Keep Your Personal Data Secure

We have implemented security measures to prevent your personal data from being accidentally or illegally lost, used or accessed by those who do not have permission. These measures include:

- access controls and user authentication
- internal IT and network security
- regular testing and review of our security measures
- staff policies and training
- incident and breach reporting processes
- business continuity and disaster recovery processes

For further information about our security measures, please see the section titled “Security Measures” in the legal section of our Website.

If there is a breach of security which has affected your personal data and we are the controller, we will notify the regulator and keep you informed (where required under data protection law).

12. 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 purpose for which

we use your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

By law we must keep Transaction Data for six years.

We may keep Identity Data, Contact Data and certain Marketing and Communications Data (specifically, any exchanges between us by email or any other means) for up to six years after the end of our contractual relationship with you or your organisation to help us bring or defend any legal proceedings.

If you are not a customer and you browse our Website, we keep personal data collected through our analytics tools.

If you are not a customer and you have asked for information from us or you have subscribed to our mailing list, we keep your details until you ask us to stop contacting you or your email address becomes permanently unavailable.

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

13. 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 continue 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 legal@immersivelabs.com.

It is usually free for you to exercise your rights and we aim to respond within one month from the date of receipt. We might ask you to verify your identity before we begin working on your request as part of our security measures (to keep personal data safe).

It might take us longer to deal with more complicated requests or where multiple requests are made at the same time, but we will always let you know first and will only ever extend the deadline by a maximum of two months.



The only time we charge a fee or refuse to respond is if we feel the request is unfounded or excessive, but we will always let you know and explain our decision.

If you want to make any of the right requests above, you can reach us at legal@immersivelabs.com.

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

Be Ready

Immersive is trusted by the world's largest organizations and governments, including Citi, Pfizer, Humana, HSBC, the UK Ministry of Defence, and the UK National Health Service. We are backed by Goldman Sachs Asset Management, Ten Eleven Ventures, Menlo Ventures, Summit Partners, Insight Partners and Citi Ventures.

