IMS Virtual Events Global Privacy Policy

IMS Global Privacy Policy
Summary of Recent Changes:
What's New as **February 3rd 2022**:
Last modified **February 3rd, 2022**
Effective Date: February 3rd, 2022

Contents

Introduction

Ajisko Ltd T/A Integrated Media Solutions, and its wholly-operating entities Integrated Media Solutions UK Ltd, Interpoint Technologies Ltd and On-VoIP Ltd, (" **IMS**" or "**We**", "**us**"), respect your privacy and we are committed to protecting your privacy through our compliance with this policy.
This policy describes our practices in connection with information that we collect through our IMS Event Cloud and Hospitality Cloud software platforms and applications (collectively our "**Applications**") as well as IMS's privacy practices in relation to the use of IMS's websites (such as www.imedia.ie, www.imedia.co.uk and other IMS websites that link to this policy) and external marketing activities.

This policy also describes your data protection rights, including a right to object to some of IMS's processing. The Policy does not apply to information collected by any third party, including through any third-party application or content (including advertising) that links to or is accessible from our Applications or websites.

Table of Contents

Are you a Customer, Customer Business Contact or Visitor?

This policy applies to the following classification of individuals that interact with IMS:

- **CUSTOMERS**: Customers are individuals that are employees or associates of IMS's direct customers (for example, event planners, travel buyers and meeting space providers), including customer personnel that are assigned a login ID and are authorized to access and use our Applications pursuant to an active IMS agreement, or under a temporary evaluation license, if available. Additionally, Customers include individuals who self-register to access our Applications.
- **CUSTOMER BUSINESS CONTACTS**: Customer Business Contacts are individuals that interact with our Customers through our Applications. These include our Customers' current and prospective clients, members, attendees, sponsors, exhibitors, marketing partners, hotel guests or other business contacts. For example, Customer Business Contacts include individuals that register for an event organized by a Customer, download an event-related mobile app, participate in a virtual event organized by a Customer, complete an online registration for an upcoming event being hosted on an IMS Zoom platform, complete an online survey, or make a hotel reservation using one of IMS's Applications.
- **VISITORS**: Individuals and prospective customers who interact with our Websites (for instance, to read about IMS products and services, download a white paper, or sign up for an online demo), as well as those who attend IMS marketing events (for instance, IMS CONNECT®, IMS live events and webinars) and whom we meet at a tradeshow or learn about through a referral from third parties or other external sources.

What types of personal data do our Customers collect?

Ajisko Ltd. T/A Integrated Media Solutions processes your personal information to meet our legal, statutory, and contractual obligations and to provide you with our products and services.

Our Applications are flexible and allow our Customers to collect a variety of personal data from and about their Customer Business Contacts, including name, organization, title, postal address, e-mail address, telephone number, fax number, social media account ID, credit or debit card number and other information including but not limited to dietary preferences, interests, opinions, activities, age, gender, education and occupation. We encourage Customer Business Contacts to review the Customers' privacy policies to further understand the types of data collected.

For a more detailed list of our Applications, please refer to the "*What are IMS's Products*" section at the end of this Privacy Policy. IMS's use of personal information collected through our Applications shall be limited to the purpose of providing the service for which our Customers have engaged IMS, to improve our services, or as required or permitted by law.
If you do not agree with our policies and practices, you may choose not to use our Applications.

How do our Customers collect personal data?

Customers can use our customizable Applications to collect personal data in a variety of ways as outlined in the examples below. We encourage Customer Business Contacts to review the Customers' privacy policies to further understand their methods of collecting the personal data.

- When Customer Business Contacts voluntarily and explicitly enter personal data into our Applications.
- When our Customers enter Customer Business Contacts into our Applications, when permitted, including by having a legitimate business interest or obtaining explicit consent from a Customer Business Contact.
- Automatically, as Customer Business Contacts interact with our Applications, using commonly used information gathering technologies such as cookies. For additional information about these technologies, see the section below titled "*How does IMS use cookies and similar technologies?*".

How do our Customers use personal data?

If a Customer Business Contact chooses to use our Applications to conduct business with a Customer (for example: register for or check into an event, respond to an online survey, download a mobile application, or send or respond to a Request for Proposal ("RFP")), any information provided in connection with that interaction will be transferred to, and under the control of, the Customer.
Customers will also have access to information (including personal data and Application usage data) related to how Customer Business Contact interact with the Applications they use. In such instances, the Customers act as data controllers towards the Customer Business Contact, under the European Economic Area ("EEA") data protection laws. Therefore, IMS cannot and does not take responsibility for the privacy practices of Customers.
The information practices of our Customers are governed by their privacy policies. We encourage Customer Business Contacts to review the Customers' privacy policies to understand their practices and procedures.

Does IMS use or sell personal data collected by our Customers?

IMS does not use personal data of our Customer Business Contacts for any purposes other than to provide services that our Customers have contracted us to provide through our Applications, as noted below, to improve our services, or as required or permitted by law. IMS does not sell personal data of our Customer Business Contacts.

How does IMS collect and process personal data from our Customers and their Customer Business Contacts?

We collect personal data from our Customers in order to facilitate communication and delivery of the Applications that our Customers are interested in or contract us to provide. For example, we may collect Customer contact information, whether through the execution of a contract, use of our services, a form on our website, queries submitted to our chat agent, an interaction with our sales or customer support team, sign up for an event, or a response to one of our surveys or marketing emails. We may also collect credit card information (e.g., credit card number and expiration date, billing address, etc.) or other customary bank information needed for billing and payment purposes.

We may record Customer telephone (or video) calls made to our Client Services team for legitimate business interests related to providing Customer support, compliance with laws, training, and quality assurance. Where required by law, we will obtain consent from Customers before proceeding with

the recorded telephone or video call. We retain such recordings until 90 days after the date of recording unless otherwise needed for contract implementation or further employee training.

We and our vendors collect Customer usage information about how our Customers interact with our Applications. This includes which webpages you visit, what you click on, when you perform certain actions, what language preference you have, what you buy, and so on.

We process Customer's and their Customer Business Contacts' personal data in the following manner:

- To disclose to our subsidiaries and affiliates for the purpose of providing services to our Customers and their Customer Business Contacts.
- To disclose to contractors, service providers, and other third parties as reasonably necessary or prudent to provide, maintain and support our Applications for our Customers and their Customer Business Contacts, such as, for example, payment processors and data center or Web hosting providers. IMS **does not share, sell or trade any information with such third parties for any promotional purposes.**
- To deliver the services that our Customer has contracted us to provide through our Applications. Some examples include:
    - If a Customer Business Contact uses one of our Applications to register for an event, we will use their provided e-mail address to send them information and announcements relating to that event.
    - If a Customer Business Contact uses one of our Applications to pay for event registration fees or other products and services using their credit cards, we will pass the credit card information to payment card processors to validate the payment information and complete the transactions.
    - When a Customer submits an RFP to a meeting space provider listed on the IMS Supplier Network, or to a Customer's Business Contact as directed by the Customer, IMS will contact that venue, management company or Customer Business Contact and disclose information, which contains personal data, necessary for it to respond to the RFP.

    - When a Customer or Customer Business Contact uses their social media credentials to share information on their social media platform or to log into one of our

Applications, we will share information with their social media account provider. The information we share will be governed by the social media site's privacy policy.

- To disclose to event organizers, exhibitors, or other attendees, as directed by a Customer or consented to by a Customer Business Contact, such as by consenting to having an exhibitor scan their event badge to share their contact information, opting-in or, clicking to give consent to receive exhibitor information, or actively consenting to share information in a IMS Application (e.g., name, contact information, profile picture, survey responses, Q&A features, comments, messages, poll responses, etc.).
- As instructed by Customer, to connect Customer Business Contacts with one another by relying on matching algorithms to recommend compatible Customer Business Contacts for optional business networking.

- To deliver to a third party in the event of a merger, divestiture, restructuring, recapitalization, reorganization, dissolution or other sale or transfer of some or all IMS's assets, whether as a continuing operating business or as part of bankruptcy, liquidation or similar proceeding, in which personal data held by IMS about our Customers and Customer Business Contacts is among the assets transferred.
- For our internal business purposes that include administering access and use of our Applications, data analysis, securely identifying Customers upon logging onto an Application, enhancing or modifying our Applications, determining the effectiveness of our promotional campaigns, billing for Services, and operating our business.
- As we believe to be necessary or appropriate: (a) under applicable law, including laws outside your country of residence; (b) to respond to requests from public and government authorities including public and government authorities outside your country of residence; and (c) to protect against or identify fraudulent transactions.
- For other purposes when Customer Business Contacts provide explicit consent.

We aggregate information about (i) Customers and Customer Business Contacts, and (ii) the use of our Applications in order to improve our Applications and to create benchmark and other business intelligence products. None of the aggregated information contains personal data (i.e., does not identify any individual).

Data Flow

- **Zoom Event** – Attendee inputs request data into Zoom registration page, the Data Processor run a registration report daily for one week in advance of the live event (unless otherwise requested by the client), which is then shared with the client using SharePoint.
- **Zoom Mailshot** – Client completes an online Mailshot Request Form, this is accessible via Jot Form, the mailshot request is then processed by IMS Virtual Events on the Mailchimp platform and issues on behalf of the Client.
- **Zoom Reports** – Following a live event, IMS process the Zoom reports and recordings including Registration / Attendee / Performance / Polls / Q&A / Survey. A copy of each report and the event recordings is shared with the client via SharePoint.

What is the legal basis for IMS to process personal data?

For individuals that are from the European Economic Area (EEA) or other regions that stipulate a lawful basis for processing personal information (such as under GDPR Article 6), our legal basis for collecting and using their personal information will depend on the nature and circumstances of the processing activity. Where we are the processor for our Customers, our legal basis may be fulfilment of a contract or consent. Where we are the controller, our legal basis will be consent or legitimate interest where the processing is in our, legitimate interests and not overridden by the individual's data protection interests, or fundamental rights and freedoms. These interests are to provide individuals with access to the Applications and features of the Applications; to send them information they have requested; to ensure the security of our Applications by trying to prevent unauthorised or malicious activities; or to enforce compliance with our terms of use, contracts and other policies.

How long does IMS store personal data collected by our Customers?

Unless otherwise provided in our contract with our Customer, we process the data until 6-months after the termination of the contract, at which time we remove it from our production environment. Within 12 months, we remove the data from our backup media.

How can a Customer Business Contact access, correct or delete their personal data?

In various countries, including countries in the EEA, as well as in some U.S. states, upon their request, Customer Business Contacts have the right to access their personal data and, if necessary, have it amended, deleted or restricted. Customer Business Contacts can also ask for some types of personal

data to be delivered to them, or another organization they nominate, in a structured and machine-readable format.

Where we process your personal data on the basis of your consent, you have the right to withdraw your consent. See the IMS contact section below. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Customer Business Contacts in the EEA also have the right to complain to a supervisory authority for data protection in the country where they live, or where they work – although we hope that we can assist with any queries or concerns you have about our use of your personal data.

IMS processes Customer Business Contacts' data under the direction of our Customers and has no direct control or ownership of the personal data we process. Customers are responsible for complying with any regulations or laws requiring notice, disclosure or obtaining consent prior to transferring the data to IMS for processing purposes. Any Customer Business Contact that seeks to access, correct or delete data, should direct their query to the Customer. If the Customer requests IMS to remove the personal data of a Customer Business Contact to comply with data protection regulations, IMS will process this request within the required time under the applicable regulation or law.

We will not accommodate a request to change information if we believe the change would violate any law or legal requirement or cause the information to be incorrect. In such instances, we will inform the Customer about the legal obligations that prevent us from fulfilling the request.

How can a Customer access, correct, or delete their personal data?

Customers have the same rights to access, correct or delete their personal data as outlined above.

Any Customer can access, correct or delete their data, or their Customer Business Contact data by submitting a request on our website at www.imedia.ie/personal-data-requests/IMS will process this request within the required time under the applicable regulation or law

We will not accommodate a request to change information if we believe the change would violate any law or legal requirement or cause the information to be incorrect. In such instances, we will inform the Customer about the legal obligations that prevent us from fulfilling the request.

We will maintain an audit history of any requests to access, correct or delete personal information to maintain a record of compliance with regulatory requirements.

There are a number of different aspects to the right of access under Article 15 GDPR.

- Individuals are entitled to confirmation of whether the controller is processing any of their personal data, which means any information which concerns or relates to them. Where that is the case, they are also entitled to a copy of their personal data.
- Individuals are entitled to other additional information about the processing of their personal data. The additional information individuals are entitled to includes: the purposes of the processing; the categories of personal data processed; who the personal data are shared with; how long the personal data will be stored; the existence of various data subject rights; the right to lodge a complaint with the DPC; information about where the data were collected from; the existence of automated decision-making (such as 'profiling'); and the safeguards in place if the personal data are transferred to a third country or international organisation.

This information is collected and used for the purposes disclosed in this Privacy Policy. IMS may have disclosed a Customer's or Visitor's, name, title, or business contact information to host venues (e.g., restaurant or hotel) or event sponsors of IMS marketing events in the 12 months immediately preceding the posting of this updated privacy policy.

If a Customer or Visitor wishes to have their information excluded from this type of disclosure, click here to submit the request. IMS may have disclosed any of the above categories of personal information pursuant to an individual's consent or under a written contract with a service provider for a business purpose in 12 months immediately preceding the posting of this updated privacy policy.

How does IMS use cookies and similar technologies?

Cookies and Web Beacons

We and our authorized third parties use cookies or similar automatic data collection technologies as individuals interact with our Applications to collect certain information about their equipment, browsing actions and patterns, including:

- Details of your visits to our Applications, such as the date and time you access our Applications, length of time you spend on our Applications, websites that linked to our

Applications or websites linked from our Applications, the resources and content that you access and use on the Applications.

- Information about your computer and internet connection, such as your IP Address, computer type, screen resolution, language, Internet browser type and version.

Below are the technologies we use for automatic data collection. We do not use any of these technologies to collect information from Customer Business Contacts for marketing or advertising purposes. Our Customers may add cookies or other similar technologies through our Applications for their own purposes, including for marketing purposes.

- **Browser Cookies.** A cookie is a small file placed on a computer hard drive. Web browsers can be configured to restrict or entirely block cookies, to configure cookie notification settings and/or to delete cookies already present on the browser or device. Information on how to do this is provided by the web browser's help/reference section. Limiting or restricting certain types of cookies may prevent a Customer or Customer Business Contact from using certain portions of our Applications, depending on how the browser settings are configured. For example, event registration cannot be completed successfully if cookies are disabled in the web browser. Unless the browser setting has been adjusted so that it will refuse cookies, our system will issue cookies when the browser interacts with our Applications. For more information about cookies and how to disable them, see https://www.safeireland.ie/cookies/.
- **Duration.** Browser Cookies are either "session" or "persistent" in duration. A "session" cookie lasts for a single browser session only and is deleted when the user closes the web browser. Session cookies allow website operators to link the actions of a user during a browser session. A "persistent" cookie remains on the user's device (even while powered off) until it expires or is deleted. A persistent cookie will be reactivated when a user returns to the website which posted the cookie. We use persistent cookies to help customize your web experience when you return to a web page or our website.

  Neither of these cookies can read or access other cookies or any data from a user's hard drive. Further, neither of these cookies alone will personally identify a user; however, a cookie will recognize a user's individual web browser or device through an IP Address, browser version, operating system and other information, and individuals who log in to their IMS accounts will be individually identifiable to particular Applications using session cookies.
- **Purpose**. Our website uses cookies that serve the following purpose types:

- **Strictly necessary (essential)**. Strictly necessary cookies make our website work, they are essential for the website to perform its basic functions.
- **Performance**. Also known as "statistics cookies", and including analytics cookies, performance cookies collect information about how you use a website, like which pages you visited and which links you clicked on. None of this information can be used to identify you. Their sole purpose is to improve website functions. This includes cookies from third-party analytics services as long as the cookies are for the exclusive use of the owner of the website visited.
- **Functionality**. Also known as "preferences" cookies, these cookies allow a website to remember choices you have made in the past, like what language you prefer. They are used to enhance the user experience of the website but are non-essential to their use, but without these cookies, certain functionality may become unavailable.
- **Marketing**. These cookies track your online activity to help advertisers deliver more relevant advertising or to limit how many times you see an ad. These cookies can share that information with other organizations or advertisers. These are persistent cookies and almost always of third-party provenance.

- **Web Beacons.** Pages in our Applications and our e-mails will contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags and single-pixel gifs). Web beacons differ from cookies in that the information is not stored on your hard drive, but invisibly embedded on web pages or in email. Web beacons permit us to track online movements of web users, for example: to count users who have visited those pages or opened an e-mail and for other related website statistics (for example, recording the popularity of certain website content and verifying system and server integrity). This enables IMS to provide a website experience more tailored to our users' preferences and interests.

At this time, we do not respond to browser 'do not track' signals, as we await for a uniform standard put forth by regulators or the privacy industry. IMS earnestly considers an individual's independent right to determine how their personal data is processed and continues to monitor developments in this area.

Advertising

We also use third parties (such as LinkedIn, Google , YouTube) to serve advertisements that may be of interest to you on other websites. For more information and the ability to control your preferences, please visit:

https://policies.google.com/privacy/partners
https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out
https://account.microsoft.com/privacy/ad-settings/signedout
https://www.facebook.com/ads/preferences/
https://twitter.com/settings/personalization

If you are located in Switzerland or the European Union, please click here

Third Party Analytics Providers

Media

Visitors to the website can download and extract any location data from images on the website.

Embedded content from other websites

Articles on this site may include embedded content (e.g. videos, images, articles, etc.). Embedded content from other websites behaves in the exact same way as if the visitor has visited the other website.

These websites may collect data about you, use cookies, embed additional third-party tracking, and monitor your interaction with that embedded content, including tracking your interaction with the embedded content if you have an account and are logged in to that website.

Analytics & Advertising

Third-party links

Occasionally, at our discretion, we may include or offer third-party products or services on our website. These third-party sites have separate and independent privacy policies. We, therefore, have no responsibility or liability for the content and activities of these linked sites. Nonetheless, we seek to protect the integrity of our site and welcome any feedback about these sites.

Google

Google's advertising requirements can be summed up by Google's Advertising Principles. They are put in place to provide a positive experience for users. https://support.google.com/adwordspolicy/answer/1316548?hl=en

We use Google AdSense Advertising on our website

Google, as a third-party vendor, uses cookies to serve ads on our site. Google's use of the DART cookie enables it to serve ads to our users based on previous visits to our site and other sites on the Internet. Users may opt-out of the use of the DART cookie by visiting the Google Ad and Content Network privacy policy.

We have implemented the following:

We, along with third-party vendors such as Google use first-party cookies (such as the Google Analytics cookies) and third-party cookies (such as the DoubleClick cookie) or other third-party identifiers together to compile data regarding user interactions with ad impressions and other ad service functions as they relate to our website. We also use the Facebook Pixel (facebook.com/policy.php) and the LinkedIn Insight Tag (https://www.linkedin.com/legal/privacy-policy) for advertising purposes.

Opting out

Users can set preferences for how Google advertises to you using the Google Ad Settings page. Alternatively, you can opt-out by visiting the Network Advertising Initiative Opt Out page or by using the Google Analytics Opt Out Browser add on.

Controlling Cookies

If you are visiting our website from the EU/EEA, then we do not set non-essential cookies unless you accept all cookies on the "cookie banner" that launches when you land on our website.

You can learn about how you can adjust your browser's settings to limit or disable non-essential cookies and other tracking technologies by visiting the section above titled "***Third Party Analytics Providers***." Strictly necessary cookies cannot be disabled.

How does IMS process data from Visitors?

IMS processes Visitor data separately and distinctly from the way we process Customer and Customer Business Contact data. By visiting our websites, attending IMS marketing events or providing us with your personal information, Visitors consent to the collection, processing and storage of their personal information as described in this section.

Visitor Personal Data Collected

IMS collects personal data including name, title, postal address, e-mail address, telephone number, , company information (including financial and billing information when purchasing IMS services), survey responses, message board posts, chat messages, contest entries and promotional enquiries. We may collect this Visitor information through a form on our website, queries submitted to our chat agent, an interaction with our sales or customer support team, when signing up for an event, or a through a response to one of our surveys or marketing emails. We use this information to provide you with additional details about our services, conduct research, provide whitepapers or to contact you after your visit.

We also collect personal data from third party sources, such as public databases, joint marketing partners, and social media platforms. For example, if a Visitor elects to connect her social media account to her account for our websites, certain personal data from the social media account will be shared with us, which may include personal data that is part of the Visitor's profile or her friends' profiles.

If you elect to do so, when you provide a reference, we collect personal information about your contacts, such as:

- Name
- Work email
- Organization
- Phone number
- City of residence

- Eircode

When you provide us with personal information about your contacts we will only use this information for the specific reason for which it is provided.

If you believe that someone else has provided us with your personal information and you would like to request us to remove it from our database, please submit a request at http://imedia.ie/personal-data-requests. Additionally, we and our analytics service providers collect personal data from cookies and similar technologies to collect information about the pages Visitors view, links Visitors click on, Visitors' web browser information, Visitors' IP address and other actions Visitors may take when accessing our websites. For additional information about our use of these technologies and how to control them, see "*Cookies and similar technologies*" section above.

IMS's Use of Visitor Personal Data Collected

IMS processes Visitor personal data to:

- Analyse how our websites are accessed;
- Personalize your browsing experience and present products or features that may be more applicable to you;
- Identify website technical problems;
- Discover, investigate, and remediate fraudulent or illegal activity;
- Transmit notices related to product, service, or policy changes;
- Respond to your product and service inquiries;
- Send you information such as product announcements, newsletters, whitepapers, other relevant offers, and upcoming promotions or events (where required, dependent on jurisdiction, we will seek and obtain your explicit consent before sending marketing emails);
- Plan and host IMS corporate events, host online forums and social networks in which Visitors may participate;
- Analyse and identify new prospects;
- Create tailored advertising, sales and promotional programs; and
- Bill customers for our services and assess the financial capability of prospective customers to afford IMS's solutions.

If you wish to remove yourself from marketing communications from IMS, please click here: https://www.imedia.ie/subscriptionmanagement.

Storing of Visitor Personal Data

Where we process Visitor personal data for marketing purposes or with Visitor consent, we process the data until the Visitor asks us to stop. It typically takes up to 30 days to implement your request. We also keep a record of when Visitors have asked us not to send direct marketing or to process Visitor data indefinitely so that we can respect the Visitor's request in the future.

Sharing of Visitor Data

IMS may share information with third party service providers contracted to provide services on our behalf as well as third parties who resell IMS services.

IMS may also engage with business partners to jointly offer products, services or other programs such as webinars or whitepapers and from time to time, we may share personal data if you purchase or show interest in any jointly offered products or services.

IMS will only share personal data of Visitors or Customers who attend a IMS marketing event with third parties if a) the Visitor explicitly consents, b) the Visitor permits their badge to be scanned, or c) it is permissible under applicable law.

Access, correct or delete Visitor data

Visitors have the same rights to access, correct or delete their personal data as do our Customers, as outlined in section "*How can a Customer access, correct or delete your personal data?*"

Any Visitor that seeks to access, correct or delete data, can do so by submitting a request on our website at https://www. IMS.com/personal-data-requests. IMS will process this request within 30 days.

We will not accommodate a request to change information if we believe the change would violate any law or legal requirement or cause the information to be incorrect. In such instances, we will inform the Visitor about the legal obligations that prevent us from fulfilling the request.

We will maintain an audit history of any requests to access, correct or delete personal information to maintain a record of compliance with regulatory requirements.

Cookies and similar technologies

All practices related to cookies and their usage described in section "*How does IMS use cookies and similar technologies"* also applies to Visitors when they interact with our websites.

Does IMS process information of children under the age of 16?

None of our Applications are directed to children under 16 years of age. We do not directly solicit or knowingly collect personal data from children under 16. If we learn that we have inadvertently collected personal information from children under the age of 16, we will delete as soon as practicable.
This Privacy Policy does not apply to the practices of our Customers with which your child may interact. You should review the applicable terms and policies for Customers to determine their appropriateness for your child, including their data collection and use practices.

Where does IMS transfer the personal data it processes?

To facilitate our business practices and delivery of our services, personal data may be collected, accessed from, transferred to or stored in the United States or in other countries where we operate, including countries outside the European Economic Area (EEA). Personal data may be accessed by IMS personnel providing services in any country where we have facilities or in which we engage third party service providers (processors or sub processors), including India, Australia and Singapore. In instances where we transfer personal data outside the European Economic Area, we implement safeguards to ensure an adequate level of data protection, such as use of Standard Contract Clauses as approved by the European Commission or taking other measures to ensure an adequate level of data protection under EU law.

How does IMS secure the data it processes?

We use a variety of organizational, technical and administrative measures to protect personal data within our organization. We follow generally accepted standards to protect the personal information

submitted to us, both during transmission and once it is received. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of any account you might have with us has been compromised), please immediately notify us of the problem by contacting us in accordance with the "*Contact*" section below.

IMS as a Data Controller

In the course of its daily organisational activities, IMS acquires, processes and stores personal data in relation to living individuals. To that extent, IMS is a Data Controller, and has obligations under the Data Protection legislation, which are reflected in this document. In accordance with Irish Data Protection legislation, this data must be acquired and managed fairly.

IMS is committed to ensuring that all staff have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the Data Protection Officer (DPO) is informed, in order that appropriate corrective action is taken.
Due to the nature of the services provided by IMS, there is a regular and active exchange of personal data between IMS and its Data Subjects. In addition, IMS exchanges personal data with Data Processors on the Data Subjects' behalf. This is consistent with IMS's obligations under the terms of its contracts with its Data Processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a staff member is unsure whether such data can be disclosed. In general terms, the staff member should consult with the Data Protection Officer to seek clarification.

Data Subject Access Requests

As part of the day-to-day operation of the organisation, IMS staff engages in active and regular exchanges of information with Data Subjects. Where a valid, formal request is submitted by a Data

Subject in relation to the personal data held by IMS which relates to them, such a request gives rise to access rights in favour of the Data Subject.

There are specific timelines within which IMS must respond to the Data Subject, depending on the nature and extent of the request. These are outlined in the attached Subject Access Request process document.

IMS staff will ensure that such requests are forwarded to the Data Protection Officer in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than 40 calendar days from receipt of the request.

Implementation

As a Data Controller, IMS ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation through the Data Processor Agreement. Regular audit trail monitoring is done by the Data Protection Officer to ensure compliance with this Agreement by any third-party entity which processes Personal Data on behalf of IMS. Failure of a Data Processor to manage IMS data in a compliant manner will be viewed as a breach of contract and will be pursued through the courts. Failure of IMS staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

We employ the following measures to restrict the availability of the Contracting Authority's information and client information:

1. **Strong passwords –** Access to software and files is via strong non-shareable passwords.
2. **Secure networks -** Network security is crucial inside and outside the office. We ensure that our system is secure when accessing sensitive information. We use a firewall, password protected network and a VPN to keep data secure.
3. **Awareness -** Cybersecurity should be a top priority when handling sensitive information. Hackers create new and innovative threats every day, while poorly trained staff can 'let slip' information that is client confidential. We therefore educate all of our staff on the need to maintain strict confidentiality even within the office environment to protect our clients' interests.

What are IMS's Virtual Events Products?

IMS Meetings & Events

- IMS Event Management
- Zoom Meetings
- Zoom Webinar
- Zoom Events
- SharePoint

How Can a Customer or Visitor Manage their IMS Email Preferences?

If you wish to update your email preferences to tailor the topics you are most interested in receiving, or to unsubscribe from communications from IMS, you may do so here: https://www.imedia.ie/subscriptionmanagement.

How to contact IMS Virtual Events regarding Data Protection.

For details regarding any privacy questions related to the IMS Virtual Events Privacy Policy, please email dpo@imedia.ie . Feel free to also contact IMS Virtual Events regarding details of our implementation of our privacy programme at:

IMS Representative

1st Floor Ashbourne Hall

Ashbourne Business Park

Dock Road, Limerick

V94 NPE0

How does IMS publicize changes to its Privacy Policy?

We will update this Privacy Policy to reflect changes to our information practices. If we make any material changes we will notify you by means of a notice on this website thirty (30) days prior to the

changes becoming effective, or by email (sent to the e-mail address specified in your account) seven (7) days prior to the changes becoming effective. However, any changes to the Privacy Policy are effective immediately upon publication for new Visitors, Customers and Customer Business Contacts. We encourage you to periodically review this page for the latest information on our privacy practices. Contact us:

Contact Sales

Social media

- IMS on Facebook
- IMS on Twitter
- IMS on LinkedIn
- IMS on YouTube

IMS on Instagram

Zoom GDPR

Customer Content

Customer content is the "in-session" information you give us directly through your use of the Services, such as files, chat logs, and transcripts, and any other information you may upload while using the Services**.** Zoom uses customer content only in connection with providing the Services – we do not monitor, sell or use customer content for any other purposes.

We do not control the actions of anyone with whom you or any other Service user may choose to share information. Therefore, we cannot and do not guarantee that any customer content you or any user provides to the Services will not be viewed by unauthorized persons. Nor can Zoom control the information a user may choose to share during a meeting. Although Zoom account holders can set privacy options that limit access to certain areas of the Services, please be aware that no security measures are perfect or impenetrable and that we are not responsible for circumvention of any security measures contained on the Services. You should be cautious about the access you provide to others when using the Services, and the information you choose to share when using the Services.

Zoom's Product and Marketing Pages

Zoom generally processes personal data in two different manners using its websites and apps. First, Zoom processes personal data it obtains from the webpages or mobile application interfaces that Zoom uses to provide its Services, such as the landing page a user sees after clicking on a link to join a meeting (Zoom's "Product Pages"). Product Pages include webpages and links that are only accessible to a Zoom account holder after they login to their Zoom account. Product Pages serve only third-party cookies that are necessary for technical support and to deliver the service. There are no interest-based advertising cookies on Product Pages.

Second, Zoom processes personal data obtained from its webpages that are accessible without logging in to a Zoom account (Zoom's "Marketing Pages"). Marketing Pages, such as www.zoom.us, are designed to encourage sales of Zoom subscriptions. They tell you about our product, plans, and pricing, features, and other related information.

Like many companies, we use advertising services that try to tailor online ads to your interests based on information collected via cookies and similar technologies on our Marketing Pages. This is called interest-based advertising. You can get more information and opt-out of the use of cookies on our Marketing Pages by clicking the Do Not Sell My Personal Information link in the footer of this webpage. You will need to set your preferences from each device and each web browser from which you wish to opt-out. This feature uses a cookie to remember your preference, so if you clear all cookies from your browser, you will need to re-set your settings. For more information regarding cookies or similar technologies, please review our Cookie Policy.

Zoom Referral Program

You can use our referral program to tell others about Zoom in certain jurisdictions (where permitted under applicable law). When you do, you will be asked to provide that person's name and email so that we can contact them. We rely on you to make sure the person you are referring to us has agreed to be contacted by us. We will send a one-time email inviting them to visit a Marketing Page. Unless

that person says they want to hear more, we will only use their name and email address to send this one-time email and to maintain an activity log of our referral program where permitted by law.

How Zoom Share Personal Data

We only share personal data with companies, organizations or individuals outside of Zoom when one of the following circumstances applies:

1. With Consent

We may share personal data with companies, organizations, individuals outside of Zoom and others when we have consent from an individual (as applicable).

2. With Zoom Partners

If Zoom received your personal data from a third-party partner and you become a Customer, Zoom may disclose select personal data to that partner or their designee for the purpose of the partnership agreement; for example, to reward a referral partner from a co-sponsored event. Zoom's partners have contractually agreed to comply with appropriate privacy and security obligations.

3. For corporate transactions

We may share personal data with actual or prospective acquirers, their representatives and other relevant participants in, or during negotiations of, any sale, merger, acquisition, restructuring, or change in control involving all or a portion of Zoom's business or assets, including in connection with bankruptcy or similar proceedings.

4. For business purposes

We provide personal data to vendors and services providers to help us provide the Services and for Zoom's business purposes. Examples include public cloud storage vendors, carriers, payment processor, and service provider for managing customer support tickets. Zoom contractually prohibits such vendors from using the personal data for any reason other than to provide the contracted-for

services and Zoom contractually requires its vendors to comply with all appropriate privacy and security requirements.

5. For legal reasons

We share personal data with companies, organizations or individuals outside of Zoom if we believe that access, use, preservation or disclosure of the information is reasonably necessary to:

- meet any applicable law or respond to valid legal process, including from law enforcement or other government agencies.
- enforce applicable Terms of Service, including investigation of potential violations.
- detect, prevent, or otherwise address fraud, security or technical issues.
- protect against harm to the rights, property or safety of Zoom, our users or the public as required or permitted by law, including to help prevent the loss of life or serious injury of anyone.

For more information about data we disclose in response to requests from law enforcement and other government agencies, please see our Guidelines for Government Requests.
Data Subject Privacy Rights and Choices
Right to Correct or Update Your Information
If you would like to correct or update information that you have provided to us, please logon to www.zoom.us and update your profile.

6. Marketing Communications

You may receive marketing email communications from us where permissible. If you would like to stop receiving these communications, you can update your preferences by using the "Unsubscribe" link found in those emails.

European Privacy Rights

If you reside in the European Economic Area, you may have the right to exercise certain privacy rights available to you under applicable laws. We will process your request in accordance with applicable

data protection laws. We may need to retain certain information for record-keeping purposes or to complete transactions that you began prior to requesting any deletion.

- **Right not to provide consent or to withdraw consent.** We may seek to rely on your consent in order to process certain personal data. Where we do so, you have the right not to provide your consent or to withdraw your consent at any time. This does not affect the lawfulness of the processing based on consent before its withdrawal.
- **Right of access and/or portability.** You may have the right to access the personal data that we hold about you and, in some limited circumstances, have that data provided to you so that you can provide or "port" that data to another provider.
- **Right of erasure.** In certain circumstances, you may have the right to the erasure of personal data that we hold about you (for example if it is no longer necessary for the purposes for which it was originally collected).
- **Right to object to processing.** You may have the right to request that Zoom stop processing your personal data and/or to stop sending you marketing communications.
- **Right to rectification.** You may have the right to require us to correct any inaccurate or incomplete personal information.
- **Right to restrict processing.** You may have the right to request that we restrict processing of your personal data in certain circumstances (for example, where you believe that the personal data we hold about you is not accurate or lawfully held).
- **Right to lodge a complaint to your local Data Protection Authority.** If you are an EEA resident, you have the right to complain to a data protection authority about our collection and use of your personal data.

How to Exercise Your Rights

To exercise any of the rights above, email us at privacy@zoom.us. You may submit a request to the following address:
Zoom Video Communications, Inc.
Attention: Data Privacy Officer
55 Almaden Blvd, Suite 600
San Jose, CA 95113

Please identify yourself and specify your request. If you have a password protected Zoom account, we will use your account information to verify your identity. If not, we will ask you to provide additional

verification information. What we request will depend on the nature of your request, how sensitive the information is, and how harmful unauthorized disclosure or deletion would be.

We use commercially reasonable efforts to delete your personal data as required but retain records necessary to comply with a governmental authority or applicable federal, state, or local law. Where legally permitted, we may decline to process requests, including requests that are unreasonably repetitive or systematic, require disproportionate technical effort, or jeopardize the privacy of others.

International Transfers

Zoom operates globally, which means personal data may be stored and processed (for example stored in a data centre) in any country where we or our service providers have facilities or hold events. By using Zoom or providing personal data for any of the purposes stated above, you acknowledge that your personal data may be transferred to or stored in the United States or in other countries around the world. Such countries may have data protection rules that are different and less protective than those of your country.

If you are a resident of the European Economic Area (EEA), and your personal data is transferred outside of the EEA, we will:

- Process it in a territory which the European Commission has determined provides an adequate level of protection for personal information; or
- Implement appropriate safeguards to protect your personal information, including transferring it in accordance with applicable transfer mechanism, including the European Commission's standard contractual clauses or the Privacy Shield Framework.

Zoom complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal data transferred from the European Union, the United Kingdom, and Switzerland to the United States in reliance on Privacy Shield. Zoom has certified that it adheres to the Privacy Shield Principles with respect to such data. If there is any conflict between the policies in this Statement and data subject rights under the Privacy Shield Principles, the Privacy Shield Principles shall govern.

To learn more about the Privacy Shield program, and to view our certification page, please visit the U.S. Department of Commerce's Privacy Shield List, https://www.privacyshield.gov/list and search for Zoom Video Communications.

Zoom is responsible for the processing of personal data it receives under the Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf. Zoom complies with the Privacy Shield Principles for all onward transfers of personal data from the EU, Switzerland, and the United Kingdom including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, Zoom is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, Zoom may be required to disclose personal data in response to valid and lawful requests by public authorities, including to meet national security or law enforcement requirements.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

Under certain conditions, more fully described on the Privacy Shield website at https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint, you can invoke binding arbitration when other dispute resolution procedures have been exhausted.

Retention

We will retain personal data for as long as required to do what we say we will in this Statement, unless a longer retention period is required by applicable law. The criteria used to determine our retention periods include:

- The length of time we have an ongoing relationship with you and provide our services to you (for example, for as long as you have an account with us or keep using our services);
- Whether we have a legal obligation to keep the data (for example, certain laws require us to keep records of your transactions for a certain period of time before we can delete them); or
- Whether retention is advisable in light of our legal position (such as in regard to applicable statutes of limitations, litigation or regulatory investigations).

Customers can delete their own accounts.

Security

Zoom is committed to protecting your personal data. We use reasonable and appropriate technical and organizational measures to protect personal data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data. If you have any questions about the security of your data, please contact our security team at security@zoom.us