

## Mobi Plus Limited Privacy Policy

Date of last revision: 2022-08-30

### 1. Privacy Policy

- 1.1 Mobi Plus Limited (collectively, “**mplus**” “**we**”, “**us**”, “**ours**”) are committed to protecting the personal information of individuals whose data we process. It is important to us that you understand how we treat your personal information and we encourage you to read this privacy policy (the “**Policy**”) carefully. In this Policy, our use of the term ‘personal information’ and ‘personal data’ refers to any information that identifies, relates to, describes, or is reasonably capable of be associated with, lined or linkable to a particular individual.
- 1.2 mplus is a technology company operating in the digital advertising ecosystem. We use data analytics to help our clients (advertisers and media agencies) to advertise their ads on various websites that allow third party advertising (“**publishers**”).
- 1.3 This Policy applies to and explains how we process personal information that we collect from individuals who interact with mplus:
- (a) through our website located at [www.mplustech.io](http://www.mplustech.io) (the “**Site**”), our interactive applications, email or other digital properties;
  - (b) in connection with the services we provide to our clients (the “**Services**”). Under the Services, mplus analyses web browsing usage on publishers’ websites in order to provide our clients with the ability to improve returns on their digital advertising spend by enabling them to serve ads that are relevant to website visitors;
  - (c) as visitors to other publisher’s websites and digital properties, including advertiser sites, third party sites, and Internet-connected devices whose browsing activities we analyze as part of digital advertising campaigns;
  - (d) as mplus’s business and marketing contacts; and
  - (e) as visitors to our physical premises.

Please note, this Policy does not apply to third-party sites that may be accessible through hyperlinks on our Site. These third-party sites may be operated subject to their own privacy policies. Linking to a third-party site does not mean that we endorse the site, any products or services described on the site, or any other material contained in that site. Please read the privacy policies of any such site carefully.

- 1.4 Whenever you interact with mplus or provide information to us on behalf of another individual or entity, such as by providing or accessing personal data about another individual, you represent that you have the authority to do so. You shall have sole responsibility for any violation of privacy laws as a result of a failure to obtain any necessary consent from such individual/entity.
- 1.5 For the purposes of the General Data Protection Regulation 2016/679 and any implementing legislation (together, the “**GDPR**”), mplus is the controller of your personal information, unless you are explicitly told otherwise. mplus is a limited company registered in Ontario, Canada with

corporation number 002766684, whose registered address is situated at 77 King St West, Suite 400, Toronto, ON, M5K 0A1.

- 1.6 If you do not want your personal information to be processed as described by this Policy, please do not access, use, or otherwise interact with our Site or Services or provide your personal information to us directly. Details of how you can exercise certain choices about how we handle your personal information are described in section 10 below.
- 1.7 As our personal information handling practices change, we may update this Policy Whenever we do so, we will post the updated Policy on our Site, indicating the date of the latest revision. . We encourage you to periodically review this Policy for the latest information on our privacy practices.
- 1.8 mplus has appointed a data protection manager, who may be contacted as follows:

**Via post:**

mplus Data Protection, 77 King St West, Suite 400, Toronto, ON, M5K 0A1

[NTD – Include telephone #]

**Via Email:** will@mplustech.io

- 1.9 If you are a resident of California, please view PART 1 of the schedule to this Policy for more disclosures and information about your additional privacy rights as a citizen of California. If you are a resident of the EU or the EEA, please see PART 2 of the schedule to this Policy for details of your additional rights under the GDPR.

## **2. Categories and Sources of Personal Information and Purposes and Lawful Bases for Processing.**

We collect and process personal data of visitors to publishers' websites, visitors to our own Site, as well as business contact data relating to the account representatives of our customers and vendors, as well as visitors to our physical premises.

Under the GDPR, there are a number of legal bases that permit us to process the personal data of EU /EEA Users for the purposes stated within this Privacy Policy. Below, we describe the legal grounds that apply to our processing of personal information of EU/EEA users.

### **2.1 Users of publishers' websites**

As described above, mplus analyses web browsing usage on our clients' websites in order to provide our clients (advertisers and media agencies) with the ability to improve returns on their digital advertising spend by enabling them to serve ads that are relevant to website visitors; We use cookies and similar technologies to develop marketing insights about user preferences, sometime in combination with other data sets, in order to better match ad content with user interests.

- (a) Sources of personal information

We may place cookies or similar technologies on user devices or browsers when they visit publishers' websites. We collect and analyse the data obtained via these applications as described in sections (b) and (c) below

(b) Personal data that we collect and process

(i) mplus may collect of the following types of personal data at the user level:

- IP address, which helps us to understand the broad location of a user Device ID (when users access websites on mobile devices), such as IDFA, AAID, SHA1;
- user ID stored in a cookie placed on a user's browser;
- latitude-longitude location data;
- timestamp on accessing the website and the website URL;
- enrichment data collected about you from third parties, such as Nielsen & Eyeota; and
- Tweets & Twitter handles, made publicly available via the Twitter platform.

We will also collect information in respect of user interactions with the placed advertisement, i.e. we will know if a user clicks on it or the user's browser & operating system type. In addition, advertisers may provide us with information on what users have previously purchased from them and when, in order to make our predictions more accurate.

(ii) We place cookies and similar technologies user devices to assist with the advertising delivery process. This includes:

- a user ID cookie to support ad personalisation, which lasts for 90 days;
- an opt-out cookie to store your opt-out and consent preferences, which lasts for 90 days;
- a session cookie to see if a browser supports cookies, which lasts for 1 browsing session;
- a cookie which limits the number of ads which a given user sees, which lasts for 90 days;
- a cookie which denotes whether a user ID is synced with other partners in the ad-serving chain; and
- a cookie which supports billing and reporting.

(c) Why do we collect personal information in respect of users of publishers' websites and what are our lawful bases for collecting and processing this data?

(i) Reasons for collection

We collect user-level personal data so that users can see ads displayed on the websites they visit which we think are most relevant to them based on their browsing behaviour and interests. This enhances the user experience while at the same time making our clients' advertising campaigns more efficient and effective.

Although we do not collect information that directly identifies individual users by name or physical address, we collect your IP address and other information about you which may constitute personal data, as we may combine it with other data. For example, based on a user's historic browsing behaviour, we may map an IP address to a city or a geographical region and other information such as weather in that region, in order to predict users' future buying decisions.

For some campaigns, we or our media partners will use data analytics to predict user interests based on machine-learning techniques involving the use of algorithms. These algorithms are regularly reviewed to ensure that they are properly adjusted and error free. We and our media partners also use technology to ensure that we do not target children or vulnerable adults or collect any special categories of personal data about users.

We never make decisions or predictions based on the characteristics of one individual. Instead we usually only target population segments or groups of individuals. These segments involve aggregated user data of no less than 1,500 users, but more typically hundreds of thousands of users who may share common characteristics, such as demographics and specific interests, such as preferences for particular types of cars.

(ii) Legal bases for collection

- **For EU/EEA individuals, the following legal bases apply to our processing of personal information Consent**

mplus will not process personal information unless its publisher & advertiser partners have first obtained the users' permission to do so. Publishers usually obtain this by means of a pop-up window that enables users to manage their preferences in regard to cookie application and related data processing.

When a user visits a website with which mplus is associated, the user will see a message asking the user if the user agrees to allow the website publisher's and third-party cookies to be set on the user's device and collect information from it when the user first visits it. If the user agrees to the application of cookies, we will then ask the user whether the user consents to the processing of the information collected for each of the following purposes:

**Ad personalisation:** The personal information we collect is used to personalise ads that you see over time on other websites. We will use the personal data we collect to infer your interests and place ads that we believe may of interest to you.

**Ad selection, reporting and delivery:** We collect information about what ads are shown, how often and when and where they are shown, whether the user clicks on them and makes a purchase. This information is used to measure the effectiveness of the ads presented.

**Content delivery, selection and reporting:** We collect and analyse information about the user's interests and what content is shown, how often, when and where, and whether the user clicks on what was shown. This is done to adjust the content displayed to the user to be most relevant.

**Measurement:** We collect information on website users' use of content in combination with previously collected information. We use this data to understand and report on such use of content to our advertising clients or for mplus's internal quality assurance purposes. In the process of using data for the above purposes, mplus also employs the following technical features: (i) matching data to offline sources, (ii) linking devices and (iii) precise geographic location data.

When a user agrees to the placement of cookies by us and one or more of the identified processing activities, we will receive a message from the website where the user's selection has been made, notifying us that we have permission to set a cookie, collect information on the user's device and use it for the agreed purposes.

Please see section 6 of this Policy for details of the choices you can make regarding cookies and other user tracking technology.

- **mplus's legitimate interests in preventing fraudulent website traffic**

We also process user IP addresses in order to detect the use of internet "bots" or similar functionality intended to distort the popularity of websites and digital ads by simulating human browsing activity. If a user agrees to the placement of a cookie and consents to the processing of their personal data for one or more of the purposes described above, our ability to detect this type of fraudulent behaviour is important to ensure that the data we rely on to cater to user preferences is not distorted by false inputs. We use a third-party vendor to assess whether the IP addresses that we are processing are associated with fraudulent activity.

- **mplus's legitimate interest in analysing social trends**

We also process personal data in order to analyse trends in social media activity. This involves analysing common keywords that appear in public posts made available on the Twitter platform and producing aggregated insights from these to inform our advertisers about current social trends. We may use Twitter handles to identify trends relating to companies and popular personalities. Should a user wish to object to our processing of their personal data for these purposes, they may do so by contacting our data privacy manager using the contact details set out in paragraph 8 above. Please also see section 6 of this Policy for details of the choices you can make regarding cookies and other user tracking technology.

- (d) How long do we keep the personal information we collect from users' visits to publishers' sites?

mplus minimises the personal data it collects about users and retains the data for only for as long as is strictly necessary for it to achieve the purpose for which the data has been collected.

Raw data that mplus collects about user online activities is kept for no longer than 180 days from the date collected and is stored in a secure environment. The user-level data is either anonymised or aggregated after 180 days, which means the information is expressed only in a summary form about user behaviour representing large groups of individuals.

Anonymous data may be kept at mplus for 2 years and aggregated information relating to financial matters stored for up to 7 years for accounting and audit purposes. During the initial 180-day period, the information about user online behaviour is used to better target the ad campaigns undertaken and adjust the audience to ensure the ad is displayed to user groups that may be most interested in the product or service advertised.

The data collected as part of the ad campaign may be used to develop insight reports for mplus's clients concerning advertising trends and campaign results. These reports are based on data that is provided in an aggregated form and does not allow for the identification of individuals.

## 2.2 Visitors to our Site

### (a) Sources of personal information

We may obtain your personal information from the following sources:

- (i) from you directly (for example, through subscribing to any services offered on our Site, including but not limited to email mailing lists, interactive services, posting material or requesting services, or if you contact us); and/or
- (ii) from your device or browser;

### (b) Personal data that we collect and process

When individuals visit our Site, we may collect and process their:

- (i) name;
- (ii) username;
- (iii) email address;
- (iv) operating system;
- (v) browser type;
- (vi) cookie data (for more information on cookies, please see section 4 of the Policy) ; and/or
- (vii) IP address.

(c) Why do we collect personal information in respect of visitors to our Site and what are our lawful bases for such collection?

(i) Why we collect personal information from visitors to our Site.

We process the personal information of visitors to our site for the following purposes:

- permitting visitors to participate in interactive features of our Services;
- ensuring that the content from our Site is presented in the most effective manner for each visitor and each visitor's device;
- allowing mplus to share information in order to provide any product or service a visitor may have requested;
- assisting in the provision of support services, the management of customer records and system administration purposes;
- monitoring statistical data about our users' browsing actions and patterns, the number of visitors to our Site, the pages visited and how long users have stayed on our Site; and/or
- exchanging personal data with mplus's group companies and affiliates, for the purpose of reporting, global management, carrying out monitoring, analysing business, and any other purposes that is incidental to or connected with the foregoing purposes.

(ii) Legal bases for collection of personal information from visitors to our Site.

We consider that it is in our legitimate interests to promote our Services via our Site and to process your information for the purposes listed above. Please do not submit your information to via our Site, if you would not like us to process your personal information for the above purpose.

If you would prefer us not to process your personal data for the purposes above, please contact our data privacy manager using the contact details set out in section 8 above. Please also see section 6 of this Policy for details of the choices you can make regarding cookies and other user tracking technology.

(d) How long do we keep the personal information we collect from visitors to our Site?

We will keep and process the personal information of visitors to our Site only for as long as is necessary for the purposes for which it was collected, unless there is a legal requirement for us to keep it for longer or the data is necessary for the establishment, exercise or defence of legal claims.

### 2.3 Business and marketing contacts

We may collect personal information related to employees, directors, authorised signatories and other representatives of mplus's existing and prospective customers or vendors as well as other business and marketing contacts.

Our existing or prospective customers are typically media agencies or advertisers that engage mplus to help them improve the performance of their advertising campaigns. Our vendors include service providers that supply us with services that we use to deliver or enhance our ad personalisation and placement services.

(a) Sources of personal information

We may obtain these categories of personal information from the following sources:

- (i) the individual directly;
- (ii) a company that employs the individual if they are an employee of an existing or prospective mplus customer or vendor,
- (iii) mplus's affiliates or group companies;
- (iv) during networking events that we have either hosted, sponsored or attended; and/or
- (v) from publicly available sources (for example, the individual's company website or social media sites).

(b) Personal information from business and marketing contacts that we collect and process

- (i) We may collect the following categories of personal data relating to our existing or prospective customers' or vendors' employees, officers, authorised signatories, and other associated individuals:
  - name;
  - business address;
  - business email address;
  - business telephone number; and/or
  - job title.

(c) Why do we collect your personal data and what are our lawful bases for such collection?

**BUSINESS AND MARKETING CONTACTS**

We process the above personal data for the following purposes:

- To provide our Services to clients and receive products or services from vendors



- To establish and manage our relationships with third parties
- To learn about how our products and services are being used by our customers and others.
- To manage security, risk and fraud prevention
- To let clients and potential clients know about our products, services and events that may be of interest to them by letter, telephone or email or other form of electronic communication.
- Promote our goods and services.
- Management reporting, inc. at intra group level.

The legal bases for processing personal data for the above is our legitimate interests and the fulfillment of contracts.

If you object to our using your personal information for the above purposes please contact our data protection manager using the contact details set out in section 8. Where we use your email address to communicate marketing information to you, we will seek your prior consent where required to do so by law.

- (d) How long do we keep the personal information we collect in respect of our business and marketing contacts?

We will keep such personal information for the duration of our business relationship and once it ends, we will delete it securely unless there is a legal requirement for us to keep it for longer or the data is necessary for the establishment, exercise or defence of legal claims. Please note, in all circumstances, we will keep and process personal information in respect of business and marketing contacts only for as long as is necessary for the purposes for which it was collected.

## 2.4 Visitors to Our Premises

- (a) Sources of personal information

We may obtain your personal data from you directly via registration and CCTV placed at our offices.

- (b) Personal data that we collect and process

- (i) name;
- (ii) business contact details;
- (iii) organisation;
- (iv) image, from CCTV cameras at our premises.

- (c) Why do we collect your personal data and what are our lawful bases for such collection?

### VISITORS TO OUR PREMISES

We process the above data for the following purposes:

- To manage security, risk and crime prevention;
- To Maintain records of visitors to our premises.

The legal basis for processing personal data for the above is our legitimate interests.

(d) How long do we keep the personal data of visitors to our premises?

We keep our visitors' personal data for as long as necessary to ensure security of our office visitors and as soon as it is no longer necessary. CCTV footage is stored in back-up for 30 days, unless there is a legal requirement for us to keep it for longer or the data is necessary for the establishment, exercise or defence of legal claims.

### 3. Data sharing with third parties

We may share your personal data with third parties. Below is a chart that describes these transfers, the reasons for the transfer, and for EU/EEA Users, the legal basis for the transfer:

<b>Categories of their party recipients and what information is transferred</b>	<b>Purpose of transfer</b>	<b>Legal basis for transferring data of EU/UK users</b>
We may share your personal data with third party service providers working on behalf of Mobiplus Examples of such third party service providers include IT providers, professional advisors (such as accountants), ad verification partners, software providers, analytics companies, technical support providers service	<ul style="list-style-type: none"><li>• To fulfill our core service of placing ads and activities related thereto (such as fraud prevention),</li><li>• To assist with our internal business functions by supporting our IT systems and infrastructure, as well as the provision of data hosting and other data processing services</li><li>• To assist with cross-device tracking</li><li>• To assist with the placement and tracking of cookies and collection of data (including information about</li></ul>	<ul style="list-style-type: none"><li>• Legitimate interests</li></ul>

	preferences and other online activities),	
We transfer your credit card information to third-party payment processors	<ul style="list-style-type: none"> <li>To process credit card transactions with our clients</li> </ul>	<ul style="list-style-type: none"> <li>Fulfillment of a contract</li> </ul>
We share your information as requested by regulators or law enforcement agencies	<ul style="list-style-type: none"> <li>To respond to requests for personal data from law enforcement</li> <li>To investigate suspected cases of fraud, identity theft, abuse of payment methods or any other activity that is illegal.</li> <li>To enforce a contract against our client, or to protect the property or safety of mplus, our users or third parties.</li> </ul>	<ul style="list-style-type: none"> <li>Legal obligation</li> <li>Legitimate interests</li> </ul>
We may disclose personal data to an acquirer or purchaser of mplus or its assets.	<ul style="list-style-type: none"> <li>If mplus or all our assets are acquired by another entity, including through a sale or in connection with our insolvency, we may share your personal data with the acquiring entity.</li> </ul>	Legitimate interests
We may share Audience Segments with our clients	Optimizing advertising, measuring effectiveness, conducting market research, or providing other insights and reporting.	Consent

3.1 **Third party service providers:**

**Aggregate and de-identified or anonymous data:** We may share aggregate, anonymous or de-identified data with third parties for research, marketing, analytics or other purposes, provided that such information does not identify and cannot be used in connection with the identification of a particular individual.

#### **4. COOKIES AND OTHER TRACKING TECHNOLOGIES**

4.1 We use cookies to recognize you when you return to our Site, or in connection with our provision of the Services on publishers' websites or other digital properties, so that we can provide you with a customized experience, and we can tailor our advertising to match your online behaviour. We may also use pixels, JavaScript, log files and other mechanisms to gather information about your use of our Site or our publishers' websites or other digital properties.

4.2 **Cookies:** Cookies are alphanumeric identifiers that we transfer to your computer's hard drive through your web browser for record-keeping purposes. Some cookies allow us to make it easier for you to navigate the websites or other digital properties on which they appear, while others are used to enable a faster log-in process or to allow us to track your activities while using the applicable websites or other digital properties. Please also see section 6 of this Policy for details of the choices you can make regarding cookies and other user tracking technology.

4.3 **Clear GIFs, Pixel Tags and Other Technologies:** Clear GIFs are tiny graphics with a unique identifier, similar in function to cookies. In contrast to cookies, which are stored on your computer's hard drive, clear GIFs are embedded invisibly on web pages. We may use clear GIFs (also referred to as web beacons, web bugs or pixel tags), in connection with our Services in order to, amongst other things, track the activities of users of our Services, help us manage content, and compile statistics about usage of our Services. We and our third-party service providers also use clear GIFs in HTML emails to our customers, to help us track email response rates, identify when our emails are viewed, and track whether our emails are forwarded.

4.4 **Log Files:** Most browsers collect certain information, such as your IP address, device type, screen resolution, operating system version, and internet browser type and version. This information is gathered automatically and stored in log files.

4.5 **Third-Party Analytics:** We also use automated devices and applications, such as Google Analytics to evaluate use of our Services. We use these tools to gather non-personal information about users to help us improve our Services and user experiences. These analytics providers may use cookies and other technologies to perform their services, and may combine the information they collect about you on our Site and publishers' websites and other digital properties with other information they have collected for their own purposes. This Policy does not cover such uses of data by third parties.

#### **5. INTEREST-BASED ADVERTISING**

#### **6. Choices Related to Cookies and Interest – Based Advertising**

6.1 We and our media partners adhere to the:

- (a) Digital Advertising Alliance Self Regulatory Principles for Online Behavioural Advertising and the National Advertising Initiative (“NAI”) codes of conduct; and

(b) European Interactive Digital Advertising Alliance (“DAA”) Self Regulatory Principles for Online Advertising,

in respect of interest-based advertising and related activities. Online users who are located in the European Union should visit [www.youronlinechoices.com](http://www.youronlinechoices.com) to exercise choices in relation to such matters, including opting out of online behavioural advertising. Online users located in the US should visit [www.optout.networkadvertising.org](http://www.optout.networkadvertising.org) to opt out of online behavioural advertising. Online users located in Canada should visit <http://youradchoices.ca> to opt out of online behavioral advertising. Please note however, that opting out of interest based and / or behavioural advertising will not opt you out of all advertising, but rather only interest based and / or behavioural advertising from mplus, its media partners or its agents or representatives.

6.2 Do Not Track

Some browsers have incorporated Do Not Track (“DNT”) preferences. Most of these features, when turned on, send signals to the website you are visiting that you do not wish to have information about your online searching and browsing activities collected and used. As there is not yet a common agreement about how to interpret DNT signals, we do not honor browser DNT signals from website browsers at this time. However, you may refuse or delete cookies or use the “opt out” option available through the DAA or NAI. If you refuse or delete cookies, some of the functionality of the websites you are may be impaired. If you change computers, devices, or browsers, or use multiple computers, devices, or browsers, and delete your cookies, you may need to repeat this process for each computer, device, or browser. Please refer to your browsers’ Help instructions to learn more about how to manage cookies and the use of other tracking technologies.

6.3 Web Browser Opt Out

mplus and its media partners serve cookies in order to provide relevant advertising. Please view the chart below for additional opt out options for targeting by mplus and its media partners.

SERVED BY	OPT-OUT OPTIONS
Trade Desk / Adsvr	<a href="#">Click here</a>
Google	<a href="#">Click here</a>
Jivox	<a href="#">Click here</a>
Amazon	<a href="#">Click here</a>

Xandr/MiQ	<a href="#">Click here</a>
Liveramp	<a href="#">Click here</a>
Vizio	<a href="#">Click here</a>

Please note that opting out does not block ads, rather it stops tracking. If you have multiple internet browsers or users on the same computer or device, you will need to perform the opt-out operation for each browser, device, and/or user. If you or your privacy software deletes the opt-out cookie from your computer, browser, or device, you will need to repeat the process with each browser and for each user.

#### 6.4 Mobile Application Opt – Out

Mobile devices allow users to opt-out of the collection of usage information within their mobile apps. To opt – out of personalised interest – based advertising on your mobile devices, please take the following steps:

- On Android devices, go to Settings, and then select the option Google. On the resulting screen, select Ads, and you will see the option to opt-out of ads personalization.
- On Apple devices, go to Settings, and then select the option Privacy. On the resulting screen select Advertising, and you will see the option to turn on limited ad tracking.

[Click here for NAI mobile opt out advice](#)

#### 6.5 Location Opt-Out

By updating the location preferences on your device, or by updating the settings for individual apps, you can block the collection of location data.

#### 6.6 Multiple Devices and Browser Opt-Out

We may use cross-device mapping services in order to link devices that belong to the same user or household. Users can opt-out of the collection of information for each device and browser by taking the steps mentioned above. However, opting out of the collection of information for one device or browser will not result in you being opted-out of the collection of information for other devices or browsers. As such, you may need to opt-out of multiple devices and browsers.

#### 6.7 Please note that use of the opt-out cookie will affect our ability to provide you content and advertisements that will more effectively match your interests and may prevent us from controlling

the frequency with which you may view any particular advertisement. Please report any problems related to the opt-out process, or any complaints with regard to online behavioural advertising data and its use, to our data protection manager, using the details provided in section 8.

## 7. Security

- 7.1 We have put in place appropriate security measures designed to prevent your personal data from being accidentally lost, used, altered, disclosed or accessed in an unauthorised manner. In addition, we limit access to your personal data to those of our employees, agents, contractors and / or other third parties who have a business need to access such data. Any such party that accesses such personal data shall do so in accordance with our instructions, and shall only use the personal data for those purposes and shall be subject to duties of confidentiality.
- 7.2 Please note that while we take precautions against possible data breaches, no website or internet transmission is completely secure. Accordingly, we cannot guarantee that unauthorised hacking, data loss or other breach may occur. Your use of our Services, the Site, and / or interactive applications and other digital properties is at your own risk.

## 8. Information about children

mplus is very sensitive to the issue of the privacy rights of children and complies with the requirements of the Children's Online Privacy Act ("COPPA"). mplus does not intentionally collect information from children under 16 years of age, and children under age 16 should not submit any information to us. Neither our Site nor any other interactive applications or other digital properties owned or operated by us are developed for, or directed at, children. If we become aware that a child has provided us with information without parental consent, or a parent or guardian of a child contacts us through the contact information provided below, we will use reasonable efforts to delete the child's information from our databases without delay.

## 9. Your Choices and Rights

- 9.1 **Access, Amend and Correct:** If you wish to access personal information that you have submitted to us, to request the correction of any inaccurate information you have submitted to us, to request deletion of or object to processing of your information, please send your request to our data privacy manager, using the contact details set out in section 8. We may ask you for additional information so that we can confirm your identity.
- 9.2 **Direct Marketing.** You may always opt-out of direct marketing emails from us by following the instructions in such emails or emailing our data privacy manager, using the contact details set out in section 8. We may continue to send you transactional or service-related communications, such as service announcements and administrative messages.
- 9.3 **Complaints.** We will take steps to try to resolve any complaint you raise regarding our treatment of your personal information. You also have the right to raise a complaint with the information commissioner or privacy regulator in your jurisdiction.
- 9.4 **Additional Information for Certain Jurisdictions.** We are committed to respecting the privacy rights of individuals under all privacy laws applicable to us. Some privacy and data protection laws require that we provide specific rights and information to consumers about our processing of

their personal data. Details of the additional rights of residents of California and citizens of the European Union or who reside in the EEA are set out in the schedule to this Policy.

## 10. International Transfers

- 10.1 mplus has operations and service providers in Canada, the United States and throughout the world. Accordingly, in the process of operating our business, we and our service providers may transfer your personal information to, or access it in, jurisdictions (including the United States) that may not provide equivalent levels of data protection as your home jurisdiction. We will take steps to ensure that your personal information receives an adequate level of protection in the jurisdictions in which we process it, including through appropriate written data processing terms and/or data transfer agreements.
- 10.2 If you are in the EU/EEA, and we process your personal information in a jurisdiction that the European Commission has deemed to **not** provide an adequate level of data protection (a “**third country**”), we will implement measures to adequately protect your personal information, such as putting in place standard contractual clauses approved by the European Commission, or transferring the data to an organization that has Binding Corporate Rules approved by an EU data protection authority, or another measure that has been approved by the EU Commission as adducing adequate safeguards for the protection of personal information when transferred to a third country. You have a right to obtain details of the mechanism under which your personal information is transferred outside of the EEA; you may request such details by contacting our data protection manager, using the details set out in section 8 above.



## SCHEDULE

### ADDITIONAL INFORMATION FOR INDIVIDUALS LOCATED IN CERTAIN JURISDICTIONS

#### PART 1 PRIVACY NOTICE FOR CALIFORNIA RESIDENTS

This PRIVACY NOTICE FOR CALIFORNIA RESIDENTS supplements the information contained in the Privacy Policy of mplus and its subsidiaries (collectively, “we,” “us,” or “our”) and applies solely to visitors, users, and others who reside in the State of California (“consumers” or “you”). We adopt this notice to comply with the California Consumer Privacy Act of 2018 (“CCPA”) and other California privacy laws. Any terms defined in the CCPA have the same meaning when used in this notice.

We have collected the following categories of personal information from consumers within the last twelve (12) months:

- Category A – Identifiers

Examples: Name, postal address, Internet Protocol address, email address, Social Security number, driver's license number, passport number, or other similar identifiers.

- Category D – Commercial information

Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

- Category F – Internet or other similar network activity

Examples: Access history and information on your interaction with our application.

- Category G – Geolocation data

Examples: Physical location or movements

- Category I – Professional or employment-related information

Examples: Occupation, employer information.

- Category K – Inferences drawn from other personal information.

Examples: Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

We obtain the categories of personal data listed above from the sources described in section 2 of this Policy, and we use the data as described in section 2 of this Policy.

As described at section 3 of this Policy, we may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract.

In the preceding twelve (12) months, we have disclosed the following categories of personal information for a business purpose:

- Category A: Identifiers.
- Category D: Commercial information.
- Category F: Internet or other similar network activity.
- Category G: Geolocation data.
- Category K: Inferences drawn from other personal information.

We disclose your personal information for a business purpose to the following categories of third parties:

- Our affiliates.
- Service providers.
- Third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.

The CCPA defines a “sale” as disclosing or making available to a third-party personal information in exchange for monetary or other valuable consideration. While we do not disclose personal information to third parties in exchange for monetary compensation from such third parties, we do disclose or make available certain categories of personal information to third parties, in order to receive certain services or benefits from them (such as when we allow third party tags to collect browsing history and other information on our Sites to improve and measure our ad campaigns).

The CCPS provides consumers with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise those rights:

- Do-Not-Sell: California residents have the right to opt-out of our sale of their personal information. Opt-out rights can be exercised by residents of California by submitting a request to us online. We do not sell personal information about any data subject who we know is younger than 16 years old without opt-in consent.
- Notice before collection: We are required to notify California residents, at or before the point of collection of their personal information, with details of the categories of personal information collected and the purposes for which such information is used.
- Request to delete: California residents have the right to request, at no charge, deletion of their personal information that we have collected about them and to have such personal information deleted, except where an exemption applies. We will respond to verifiable requests received from California residents as required by law.
- Request to know: California residents have the right to request and, subject to certain exemptions, receive a copy of the specific pieces of personal information that we have collected about them in the prior 12 months and to have this delivered, free of charge, either (a) by mail or (b) electronically in a portable and, to the extent technically feasible, readily useable format that

allows the individual to transmit this information to another entity without hindrance. California residents also have the right to request that we provide them certain information about how we have handled their personal information in the prior 12 months, including:

- o categories of personal information collected;
- o categories of sources of personal information;
- o business and/or commercial purposes for collecting and selling their personal information;

California residents may make a Request to Know up to twice every 12 months, at no charge. We will respond to verifiable requests received from California residents as required by law.

1.1. Discrimination and financial incentives: The CCPA prohibits discrimination against California residents for exercising their rights under the CCPA. A business may offer financial incentives for the collection, sale or deletion of California residents' personal information, where the incentive is not unjust, unreasonable, coercive or usurious, and is made available in compliance with applicable transparency, informed consent, and opt-out requirements. California residents have the right to be notified of any financial incentives offers and their material terms, the right to opt-out of such incentives at any time, and may not be included in such incentives without their prior informed opt-in consent.

1.3 Submitting Verifiable Requests: Requests to know and requests to delete may be submitted:

- By email at to our data privacy manager, using the contact details set out in section 8 above.

We will respond to verifiable requests received from California residents as required by law. For more information about our privacy practices, you may contact our data privacy manager using the contact details set out in section 8 of the Policy.

## **PART 2 INDIVIDUALS IN THE EUROPEAN UNION / EEA**

This part explains the additional rights that data subjects in the European Union or EEA have pursuant to the GDPR.

2.1. **Rights under the GDPR**: Individuals in the EEA have the following rights with respect to their personal data.

(a) **Right of access**: You can ask us to:

- (i) confirm whether we are processing your personal information;
- (ii) give you a copy of that information; and
- (iii) provide you with other information about your personal information such as what data we have, what we use it for, who we disclose it to, whether we transfer it abroad and how we protect it, how long we keep it for, what rights you have, how you can make a complaint, where we got your information from and whether we

have carried out any profiling, to the extent that such information has not already been provided to you in this Policy.

- (b) **Right to rectify and complete personal information:** You can ask us to rectify inaccurate information. We may seek to verify the accuracy of the data before rectifying it.
- (c) **Right of erasure:** You can ask us to erase your personal information, but only where:
  - (i) it is no longer needed for the purposes for which it was collected;
  - (ii) you have withdrawn your consent (where the data processing was based on consent); following a successful right to object (see the details of certain rights to object to processing set out in paragraphs (e) and (f) below); or
  - (iii) it has been processed unlawfully; or to comply with a legal obligation to which we are subject.

We are not required to comply with your request to erase your personal information if the processing of your personal information is necessary. For example, when it is required for compliance with a legal obligation; or for the establishment, exercise or defense of legal claims. There are certain other circumstances in which we are not required to comply with your erasure request, although these two are the most likely circumstances in which we would deny that request.

- (d) **Right of restriction:** You can ask us to restrict (i.e. keep but not use) your personal information, but only where:
  - (i) its accuracy is contested, to allow us to verify its accuracy;
  - (ii) the processing is unlawful, but you do not want it erased;
  - (iii) it is no longer needed for the purposes for which it was collected, but we still need it to establish, exercise or defend legal claims;
  - (iv) you have exercised the right to object, and verification of overriding grounds is pending.

We can continue to use your personal information following a request for restriction, where: we have your consent; to establish, exercise or defend legal claims; or to protect the rights of another natural or legal person.

- (e) **Right to object to our use of your personal information for direct marketing purposes:** You can request that we change the manner in which we contact you for marketing purposes. You can request that we not transfer your personal information to unaffiliated third parties for the purposes of direct marketing or any other purposes.
- (f) **Right to object for other purposes:** You have the right to object at any time to any processing of your personal information which has our legitimate interests as its legal basis. You may exercise this right without incurring any costs. If you raise an objection,

we will have an opportunity to demonstrate that we have compelling legitimate interests which override your rights and freedoms. The right to object does not exist, in particular, if the processing of your personal information is necessary to take steps prior to entering into a contract or to perform a contract already concluded.

- (g) **Right to (data) portability:** You can ask us to provide your personal information to you in a structured, commonly used, machine-readable format, or you can ask to have it 'ported' directly to another data controller, but only where our processing is based on your consent and the processing is carried out by automated means.
- (h) **Right to withdraw consent:** You can withdraw your consent in respect of any processing of personal information which is based upon a consent which you have previously provided.
- (i) **Right to obtain a copy of safeguards:** you can ask to obtain a copy of, or reference to, the safeguards under which your personal information is transferred outside the EU/EEA. We may redact data transfer agreements to protect commercial terms.
- (j) **Right to lodge a complaint with your local supervisory authority:** You have a right to lodge a complaint with your local supervisory authority if you have concerns about how we are processing your personal information. We ask that you please attempt to resolve any issue with us first, although you have a right to contact your supervisory authority at any time.
- (k) **Submitting a GDPR Request:** Please contact our data protection manager using the details set out in section 8 of the Policy to exercise one of these rights. If we receive any requests from individuals related to the data under the control of a third party, we will forward the request to the relevant third parties.