Privacy Policy

MassMetric – Website Policy

Privacy Policy

Last Updated: January 02,2025

Please read this Privacy Notice ("Notice") carefully as it contains important information related to your Personal Data under Data Protection Laws. This Notice applies to all of our legal which are collectively referred to as the "MassMetric Group".

This Notice explains how and why we collect, store, use, and share your Personal Data. It also explains your rights related to your Personal Data, including how to contact us in the event you have a complaint.

1. Key data protection terms

Below is an explanation of key terms referred to in this Notice.

Consent:
Refers to when an individual gives agreement which is freely given, specific, informed and is an unambiguous indication of their wishes. It is done by a statement or by a clear positive action in respect of the Processing of any Personal Data relating to them.

Business: Refers to any legal entity that operates for profit in California and determines the purposes and means of the Processing of Personal Data and meets one of three thresholds outlined by the California Consumer Privacy Act 2018 ("**CCPA**") (and as amended by the California Privacy Rights Act 2023 ("**CPRA**")).

Data Controller and Data Processor: Refers to any legal entity that determines when, why and how to Process Personal Data. It is responsible for establishing policies and procedures in line with Data Protection Laws. The Data Controller is the entity (individual or organization) that determines the purposes and means of processing personal data and is responsible for ensuring compliance with data protection laws. In contrast, the Data Processor is the entity that processes personal

data on behalf of the data controller and must follow the instructions of the data controller while complying with data protection laws. A Personal Data Breach is a security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

Data Minimization and Accountability: As per data minimization personal data collected should be adequate, relevant, and limited to what is necessary for the purposes for which they are processed. Accountability is the principle that data controllers are responsible for, and must be able to demonstrate, compliance with data protection laws.

Data Protection Laws: Refers to the CCPA, CPRA, UK GDPR, UK Data Protection Act 2018, UK Privacy and Electronic Communications Regulations, the European Union's General Data Protection Regulation 2016/679 and Privacy and Electronic Communications (EC Directive) Regulations 2003 as well as any other applicable laws relating to Personal Data.

Data Subject: Refers to a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Legitimate Interest: Refers to when an organization's interests are legitimate (as they need to do something to operate) and these interests do not override an individual's interests or fundamental rights and freedoms. Lawful Basis simply means legal grounds for processing personal data, such as consent, contract, legal obligation, vital interests, public task, or legitimate interests. Individual Rights are the rights granted to individuals under data protection laws, including the right to access, rectify, erase, restrict processing, object to processing, and data portability.

Personal Data: Personal Data refers to information about an individual that can be used to identify them, such as their name, address, email, and phone number. This includes any data that can be linked to a person, even if it doesn't directly include their name. The Data Subject is the individual whose personal data is being collected, held, or processed, and this term applies to living individuals only.

Process, Processing and Processed: Refers to any activity that involves the use of Personal Data. Processing encompasses any operation performed on personal data, whether automated or manual, including collection, recording, organization, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction. Processing also includes transmitting or transferring Personal Data to third parties.

Service Provider: Refers to any legal entity that operates under a service provider contract and fulfils the following characteristics: operates for profit, receives consumers' personal information from a business and Processes the Personal Data on behalf of a business under the CCPA and CPRA.

Special Category Data: Refers to more sensitive information including that which reveals racial or ethnic origin, religious or similar beliefs, physical or mental health conditions and biometric or genetic data of an individual.

UK GDPR: The General Data Protection Regulation (GDPR) is a comprehensive data protection law in the European Union that sets out the principles and requirements for processing personal data. European Union's General Data Protection Regulation 2016/679 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419).

---

2. MassMetric categorization under Data Protection Law

Data Protection Laws have created the concepts of a Data Controller (also known as a Business) and a Data Processor (also known as a Service Provider). All of the entities within the MassMetric Group act as Data Controllers and Businesses as defined under Data Protection Laws.

The reasons for which our entities are Data Controllers are outlined below.

- We decide what to collect in respect of the Personal Data, whether it be from our websites or from third parties where we source data including Personal Data.

- We determine what the purpose and outcome of the Processing will be and do this through our bespoke and value-driven consultancy services for our customers.
- We decide which Data Subjects to collect Personal Data about and on what specifically. We do this again, through our bespoke and value-driven consultancy services whereby we engage with customers and identify how best to support them in growing their business.
- We make decisions about the Data Subjects as part of the Processing in that we determine whether those Data Subjects would find benefit and interest in a specific campaign that we are supporting our customers with at the time.
- We exercise professional judgement in the Processing of the Personal Data as we are not a data broker and instead a thought-driven consultancy service which evaluates, assesses and critically considers Personal Data that it has obtained and formulates a strategy on how to utilize relevant part of that Personal Data for the benefits of our customers and Data Subjects.
- We have complete autonomy as to how the Personal data is Processed. This is because we have built proprietary tools and determine how to operate our business and how to support and advise our customers in the best manner possible. We are not directed by our customers in how we must Process the Personal Data.

Where applicable, the MassMetric Group has registered with the appropriate data protection supervisory authorities. Examples of the authorities which govern the MassMetric Group are listed below.

- Federal Trade Commission in the United States of America ("**USA**").
- Information Commissioner's Office ("**ICO**") in the United Kingdom ("**UK**").
- The National Institute of Transparency for Access to Information and Personal Data in Mexico.

The MassMetric Group has completed a thorough assessment of its organization under Data Protection Laws and has made the decision to appoint a Data Protection Officer ("**DPO**"). The DPO overseas our data protection compliance program and responds to Data Subjects. If you would like to contact our DPO, please see **Section 20**.

The MassMetric Group has also completed a detailed analysis on whether it is required to appoint an European Union ("**EU**") representative under Data Protection Laws and has determined that it is required and would be in the benefit of EU Data Subjects. In light of this, the MassMetric Group has appointed Aria Grace Law CIC (Ireland) to be its EU representative. If you are in the European Economic Area

("**EEA**") and have any concerns relating to the Processing of your Personal Data, you may contact Aria Grace Law CIC (Ireland) by emailing it on privacy@aria-grace.com.

3. Data protection Compliance

As we believe that protecting the confidentiality and integrity of Personal Data is a critical responsibility that we must take seriously at all times, we have built a robust data protection compliance program. Our data protection compliance program includes a governance framework, record of processing of activities / data register, notices, policies and procedures, technical security controls as well as training and communications material for employees.

Our data protection compliance program is built on the following principles:

- Personal Data must be Processed lawfully, fairly and in a transparent manner.
- Personal Data must be collected only for specified, explicit and legitimate purposes.
- Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.
- Personal Data is accurate and where necessary, kept up to date.
- Personal Data should not be kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the Personal Data is Processed.
- Personal Data must be Processed in a manner that ensures its security using appropriate technical and organizational measures to protect it against unauthorized or unlawful Processing and against accidental loss, destruction or damage.

4. Personal Data from children

Our websites, services and applications (including the Byonic Platform) are not intended for children under the age of 18 without parental Consent. If you are under the age of 18 and wish to seek a consultation through our websites, your parent or legal guardian must create the account, submit your Personal Data, and confirm their understanding of this Notice on your behalf.

If you are under the age of 13, you may only use our services and access our websites with the supervision and Consent of your parents or legal guardians. If we learn that we have collected Personal Data from someone under the age of 13 that was not provided with the supervision and consent of the minor's parents or legal guardian, we will promptly delete that information. If you believe we have

impermissibly collected Personal Data from someone under the age of 13, please contact us using the information in **Section 20**.

5. Personal Data We Collect

(a) Applicants for employment

Personal Data Categories	**Examples of Personal Data Processed**
Identification Data (including Special Category Data under some Data Protection Laws)	• Name • Address • Telephone number • Email address • Social security number (if in the USA) • Social insurance number (if in Canada) • Government identification number (where applicable) • Drivers license number (where applicable) • Passport number and information • Date of birth
Special Category Data	• Disability, biometric (such as photographs and video footage) and genetic information where you choose to provide it as part of the recruitment process (such as in order to inform of us of any reasonable adjustments that we need to put in place during the interview process)
Pre-Employment Data	• Background screening information (including checks on criminal offences and convictions, credit,

	toxicology and past employment checks) • Academic and professional qualifications and certificates (including dates) • Current and past employers (including dates)
Technical and Usage Data	• Internet protocol ("IP") address (if you are submitting your application via our website) • Google Advertiser ID or other identifiers for advertising • Browsing history on our website, application or advertisement • Search history on our website, application or advertisement

(b) Potential and existing customers

Personal Data Categories	**Examples of Personal Data Processed**
Identification Data (including Special Category Data under some Data Protection Laws)	• Name • Address • Telephone number • Email address • Online account name
Financial Data	• Bank account details • Tax numbers • Invoices
Invoices	• IP address • Google Advertiser ID or other identifiers for advertising

	• Browsing history on our website, application or advertisement • Search history on our website, application or advertisement

(c) Generated leads

We need to Process Personal Data on Data Subjects in order to be able to provide our services to our customers. Below is a list of the Personal Data that we collect and is required for generated leads, in order for us to subsequently provide qualified lead data ("**Qualified Lead**") to our customers.

Personal Data Categories	**Examples of Personal Data Processed**
Identification Data (including Special Category Data under some Data Protection Laws)	• Name • Address • Telephone number • Business email address • Employer information • Job title • Job function
Technical & Usage Data	• IP address • Google Advertiser ID or other identifiers for advertising • Browsing history on our website, application or advertisement • Search history on our website, application or advertisement • Uniform Resource Locators ("URLs") to and data from social media profiles

We collect, store, and provide Qualified Lead data to customers if you have Consented to us to do so only. In countries that require double opt-in consent (e.g., Austria, Germany, Greece, Switzerland, Luxembourg, and Norway), we collect,

store, and provide Qualified Lead data to customers only if you have doubly Consented to us to do so.

(d) Website visitors

Personal Data Categories	**Examples of Personal Data Processed**
Identification Data (including Special Category Data under some Data Protection Laws)	• Name • Address • Telephone number • Email address • Online account name
Technical & Usage Data	• IP address • Google Advertiser ID or other identifiers for advertising • Browsing history on our website, application or advertisement • Search history on our website, application or advertisement

(e) Potential and existing third-party suppliers

Personal Data Categories	**Examples of Personal Data Processed**
Identification Data (including Special Category Data under some Data Protection Laws)	• Name • Address • Telephone number • Email address • Online business account name
Financial Data	• Bank account details • Tax numbers • Invoices
Technical & Usage Data	• IP address

	• Google Advertiser ID or other identifiers for advertising • Browsing history on our website, application or advertisement • Search history on our website, application or advertisement

6. Legitimate Interest Basis

Under Data Protection Laws, we can only use your Personal Data if we have a proper legal reason for doing so.

Data Subject type	**Legal reasons**
Applicants for employment	• For the performance of our contract with you or to take steps before entering into a contract with you. • For our Legitimate Interests or those of a third party. • Where you have given Consent.
Potential and existing customers	• For the performance of our contract with you or to take steps before entering into a contract with you. • For our Legitimate Interests or those of a third party. • Where you have given Consent. • To comply with our legal and regulatory obligations.
Generated leads	• For our Legitimate Interests or those of a third party. • Where you have given Consent.
Website visitors	• For our Legitimate Interests or those of a third party. • Where you have given Consent.

Potential and existing third-party suppliers	• For the performance of our contract with you or to take steps before entering into a contract with you. • For our Legitimate Interests or those of a third party. • Where you have given Consent. • To comply with our legal and regulatory obligations.

7. Method of Personal Data Collection

We collect most Personal Data directly from you when you provide such information directly to us and when such information is collected in connection with your application for employment, through our lead generation techniques – in person, by telephone, text, email, web applications, and/or via our websites.

Other sources from which we may collect your Personal Data are outlined below.

- From publicly accessible sources (e.g., property records).
- Directly from our third-party suppliers (e.g., background screening providers).
- Our subsidiaries and affiliates.
- From cookies on our website (see **Cookies Notice** here)hyper link to Cookie Policy
- From our Information Technology ("IT") systems, including automated monitoring of our websites, Artificial Intelligence enabled tools and other technical systems, such as our computer networks and connections, communications systems, email and instant messaging systems, and security systems.
- We may use public/ social media / third party sources to complete any incomplete data that was collected by website or AI tools.

8. Personal Data Storage

Personal Data may be held at our offices and those of our representatives, agents, and third party suppliers including Service Providers. For generated leads, your Personal Data may also be held at the offices and technology of our customers that purchased your generated lead data.

If you are a Data Subject of the UK or EEA, the Personal Data that we collect from you and Process as a result of an application for employment, lead generation, use

of our services, or use of our websites may be transferred to, and stored at, a destination in the USA, Mexico, India, Australia or other countries. It may also be Processed by staff who work for us or our third party suppliers operating in the USA, Mexico, India, Australia or other countries.

9. Sharing of Personal Data

We routinely share Personal Data and have explained more information on who we share it with below.

Data Subject type	**Summary of third parties**
Applicants for employment	• Our third-party applicant tracking system. • Our talent acquisition team including, but not limited to, our hiring managers, operational leaders responsible for any role(s) that you have applied and for future positions that may become available, and other employees that may interview or consider you for employment for either a position that you have applied or future positions that may become available. • Service Providers necessary for pre-employment screening. • Other third parties we use to help run our business and necessary for pre-employment screening, including customers in the instance where we plan to place an employment applicant at a customer's location for a significant time. However, when we share your Personal Data with customers for pre-employment screening purposes, we only share the applicant's name and employment

	history — we do not share any Special Category Data. • Our subsidiaries and affiliates.
Potential and existing customers	• Our employees necessary to provide our services and customer support. • Service Providers necessary to provide and help deliver our services. • Other third parties we use to help run our business and necessary to provide our services and support customers. • Our subsidiaries and affiliates.
Generated leads	• Our employees to generate leads, provide leads to our customers, provide our services and customer support. • Service Providers necessary to provide and help deliver our services. • Customers if they are Qualified Leads. • Other third parties we use to help run our business and necessary to provide our services and support customers. • Our subsidiaries and affiliates.
Website visitors	• Service Providers we use to help deliver our services and maintain our website. • Other third parties we use to help us run our business, such as social media sites, search engines,

	marketing agencies or website hosts. • Our subsidiaries and affiliates.
Potential and existing third-party suppliers	• Our employees necessary to engage with you and utilize your services. • Our subsidiaries and affiliates.

Please note that we impose contractual obligations on Service Providers to ensure they only use Personal Data to provide services to us and to you. For generated leads, we also impose contractual obligations on customers to ensure they only use Personal Data shared as Qualified Leads to market, advertise, or sell to you, or in another way allowable by Data Protection Laws only.

We may also share Personal Data with the organizations listed below.

- External auditors.
- Law enforcement agencies including national security agencies.
- Courts as required by court order or required by litigation.
- Regulatory bodies to comply with our legal and regulatory obligations.

Other parties such as potential buyers of some or all of our business or during a re-structuring. In this event, we will typically anonymize information, but this may not always be possible. The recipient of this information will be bound by confidentiality obligations.

10. Process to transfer Personal Data across borders

We ensure that Personal Data is transferred safely and securely at all times. Whenever your Personal Data is transferred outside of the UK and/or the EEA, we ensure that it's protected by putting in one of the following safeguards:

- We will only transfer your Personal Data to countries that have been deemed to provide an adequate level of protection for Personal Data as endorsed by the ICO and identified and determined by the European Commission.
- We will only transfer your Personal Data where we have entered into specific contracts with an organization outside of the UK and/or the EEA which states that they will ensure that your Personal Data has the same level of protection as if it were in the UK and/or the EEA.

If you want to find out the specific mechanism used when transferring your Personal Data out of the UK and/or the EEA, please contact us using the details in **Section 20**.

11. Data Security Measures

We take appropriate measures to ensure that all Personal Data is kept secure including security measures to prevent Personal Data from being accidentally lost, or used or accessed in an unauthorized way, for the duration of your use of our services.

We limit access to your Personal Data to those who have a genuine business need to know it. Those Processing your information will do so only in an authorized manner and are subject to a duty of confidentiality.

We impose contractual obligations on Data Processors and Service Providers to ensure they only use Personal Data to provide services to us and to you. For generated leads, we also impose contractual obligations on customers to ensure they only use any Personal Data shared in Qualified Leads data to market, advertise, or sell to you, or in another way allowable by Data Protection Laws.

We have also been assessed and certified as meeting the requirements for the ISO/IEC 27001:2013 certification from 29 March 2023 through to 29 October 2025. The certification applies to customer information relating to the following: demand generation, content syndication and account-based marketing. By earning this certification, we have established an information security management system that meets high international standards.

Further to this, we have procedures in place to deal with any suspected data security breach. We will notify you and any applicable data protection supervisory authority of a suspected data security breach where we are legally required to do so.

Please note that the transmission of information via the internet is not completely secure. Although we will do our best to protect your Personal Data, we cannot guarantee the security of your Personal Data transmitted to us or our website, therefore any transmission remains at your own risk. Once we have received your information, we will use strict procedures and security features in order to prevent unauthorized access.

12. Updating your Personal Data

If your personal details change, you may update them us by contacting us at dataprotection@MassMetric.com

We will attempt to update your Personal Data within 30 calendar days of any new or updated Personal Data being provided to us, in order to ensure that the Personal Data that we hold about you is as accurate and as up to date as possible.

13. Personal Data Retention Period

We will keep your Personal Data while you have an application for employment (including employment screening) or an account with us or while we are providing services. For generated leads, we will keep your information as long as you fit our current or prospective customers' lead profile. Thereafter, we will keep your Personal Data for as long as is necessary only for the reasons outlined below.

- To respond to any questions, complaints or claims made by you or on your behalf.
- To consider applicants for other future employment opportunities that may arise.
- To show that we treated you fairly.
- To keep records required by law.

14. Data Subject Rights

The Data Subject rights that are applicable to you depend on the appropriate Data Protection Laws that are relevant to your situation. We have outlined below the Data Protection Laws and the Data Subject rights for certain jurisdictions.

(a) Data Protection Laws – UK, EU and Swiss Law

Your Right	**Summary**
Right to access	Right to access the right to be provided with a copy of your Personal Data.
Right to rectification	The right to require us to correct any mistakes in your Personal Data.
Right to be forgotten	The right to require us to delete your Personal Data—in certain situations.
Right to restriction of Processing	The right to require us to restrict Processing of your Personal Data—in certain circumstances, e.g., if you contest the accuracy of the data.
Right to data portability	The right to receive the Personal Data you provided to us, in a structured, commonly used and machine-readable

	format and/or transmit that data to a third party – in certain situations.
Right to object	The right to object at any time to your Personal Data being Processed for direct marketing (including profiling) and/or the right to object, in certain situations, to our continued Processing of your Personal Data.
Right not to be subjected	The right not to be subject to a decision based solely on automated Processing
to automated decision-making	Right not to be subjected to automated decision-making The right not to be subject to a decision based solely on automated Processing (including profiling) that produces legal effects concerning you or similarly significantly affects you.
Right to lodge a complaint	Users that reside in the UK, EEA (and Switzerland) have the right to lodge a complaint about our data collection and Processing actions with the supervisory authority concerned.

(b) Data Protection Laws – Other Jurisdictions

Your Data Subject rights under North American Privacy Laws (including but not limited to the laws of Canada, California, Colorado, Connecticut, Indiana, Iowa, Tennessee, Texas, Utah, and Virginia), under South American Laws (including Argentina, Brazil, and Colombia), under Asia-Pacific Laws (including Australia, New Zealand, China, Hong Kong, Philippines, Singapore, South Korea, Armenia, Israel, and Turkey), and under African Laws (including Benin Republic, Kenya, Nigeria, and South Africa) are covered in this **Section 14**.

While all of the above-mentioned countries and states do not have the same Data Subject rights, we provide these rights that meet or exceed the rights of these countries and states.

Your Right	**Summary**

Rights to know about and access to the Personal Data collected about you	**You have the right to know the information below.** • The categories of Personal Data we have collected about you. • The categories of sources from which the Personal Data is collected. • Our business or commercial purpose for collecting or selling Personal Data. • The categories of third parties with whom we share Personal Data (if any). • The specific pieces of Personal Data we have collected about you. **Please note that we are not required to:** • Retain any Personal Data about you that was collected for a single one-time transaction if, in the ordinary course of business, that information about you is not retained. • Re-identify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered Personal Data. • Provide the Personal Data to you more than twice in a 12-month period.
Right to correct inaccurate Personal Data collected about you	The right to require us to correct any mistakes in your Personal Data.
Rights to opt-out or limit the sale and disclosure of Special Category Data	In connection with any Personal Data we may sell or disclose to a third party for a business purpose, you have the right to know the points below. • The categories of Personal Data about you that we sold and the categories of

	third parties to whom the Personal Data was sold. • The categories of Personal Data that we disclosed about you for a business purpose. You have the right under the CCPA and CPRA and certain other privacy and Data Protection Laws, as applicable, to opt-out of or limit the sale or disclosure of your Personal Data. To opt-out of the sale or limit the disclosure of your Personal Data, click here, “Do Not Sell or Share My Personal Data” to complete our form or email us on dataprotection@MassMetric.com to exercise your rights. If you exercise your right to opt-out of the sale or limit the disclosure of your Personal Data, we will refrain from selling your Personal Data or going beyond your requested limits for disclosure of Personal Data, unless you subsequently provide express authorization for the sale of your Personal Data.
Right to deletion	**Subject to certain exceptions set out below, on receipt of a verifiable request from you, we will:** • Delete your Personal Data from our records. • Direct any Service Providers to delete your Personal Data from their record. Please note that we may not delete your Personal Data in certain circumstances including if it was necessary to complete a transaction for which the Personal Data was collected or to comply with an existing legal obligation.
Right to fair treatment and protection against discrimination	You have the right to not be discriminated against by us because you exercised any of your rights

	under the CCPA and CPRA and certain other privacy and Data Protection Laws, as applicable. This means we cannot, among other things, do the points outlined below. • Deny goods or services to you. • Charge different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties. • Provide a different level or quality of goods or services to you. Suggest that you will receive a different price or rate for goods or services or a different level or quality of goods or services. Please note that we may charge a different price or rate or provide a different level or quality of service to you, if that difference is reasonably related to the value provided to our business by your Personal Data.

(c) Exercising your -Data Subjects' rights

If you would like to exercise any of your rights as described in this Notice, please email us at dataprotection@MassMetric.com.

Please note that you may only make a CCPA and CPRA-related data access or data portability disclosure request twice within a 12-month period.

Please note that EU GDPR-related requests to exercise any rights under the EU GDPR can also be made our EU representative as explained above.

If you choose to contact us, you will need to provide us with:

- Enough information to identify you (e.g., your full name, address, and email address);
- Proof of your identity and address (e.g., a copy of your driving license or passport and a recent utility or credit card bill); and
- A description of what right you want to exercise and the information to which your request relates.

Any Personal Data we collect from you to verify your identity in connection with you request will be used solely for the purposes of verification.

(d) Data Subjects' right to complain

Data Protection Laws are constantly evolving, and we endeavor to maintain best practice. However, we recognize that we may not always get it right and if you are not satisfied in the way we handle your Personal Data, or you wish to discuss our processes, then we would like to hear from you. If there is something which we have not done correctly with
your Personal Data, then we would also appreciate the opportunity to deal with your concerns before you approach a data protection supervisory authority, so please do contact us in the first instance by using the details in **Section 20**. All complaints are taken seriously and managed by our DPO (who sits within our Legal & Compliance team).

If you are still unsatisfied with our response, you should know that you have the right to lodge a complaint with a data protection supervisory authority.

15. Do we sell Personal Data?

In the last 12 months, we have not sold Personal Data of employment applicants, customers or website visitors to any third parties that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household.

However, with your affirmative Consent, we do sell Qualified Lead information, which may include Personal Data of generated leads, to our customers. For generated leads, in the last 12 months, we have sold to one or more customers the following categories of Personal Data that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household:

- Identification Data (including Special Category Data under some Data Protection Laws)
- Special Category Data
- Technical & Usage Data
- Inferences drawn from any of the Personal Data identified above to create a profile about an individual, group of, or aggregate lead(s) and consumer(s) reflecting preferences, characteristics, psychological or other trends, predispositions, behavior, attitudes, intelligence, abilities, aptitudes or any other necessary business purpose.

16. Sharing /Disclosure of Personal Information

In the past 12 months, we could have disclosed the following categories of Personal Data to one or more third parties for business purposes. This data identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a specific employment applicant, customer, website visitor, individual, or household:

- **Identification Data**: This includes personal identifiers and Special Category Data as defined under Data Protection Laws.
- **Technical & Usage Data**: Information related to the use of our website and services, including IP addresses, browser types, and usage patterns.
- **Pre-Employment Data**: Information collected during the hiring process, such as resumes, background checks, and interview notes.
- **Inferences**: Insights drawn from the Personal Data mentioned above to create profiles about individuals, groups, or aggregated employment applicants, employees, customers, general consumers, and website visitors. These profiles may reflect preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, aptitudes, or other necessary business purposes.

17. Marketing Approach

We may use your Personal Data to send you updates or communications by email, text message, telephone or post about our services, including exclusive offers, promotions or new services. We have a Legitimate Interest in Processing your Personal Data for promotional purposes. This means we do not usually need your Consent to send you promotional communications. However, where Consent is needed, we will ask for this Consent separately and clearly.

You have the right to opt out of receiving promotional communications at any time by contacting us at dataprotection@MassMetric.com or by using the “unsubscribe” link in emails or “STOP” number in texts.

We may ask you to confirm or update your marketing preferences if you instruct us to provide further services in the future, or if there are changes in the law, regulation or the structure of our business.

18. Third-party Links

Our website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements and notices. When you leave our website, we encourage you to read the privacy documentation the website you visit.

19. Changes to Privacy Notice

This Privacy Notice was last updated in January 2025 by our DPO and it's regularly kept under review and updated as and when necessary. If you have any questions about it, please do reach out to our DPO by using the information in **Section 20**.

20. Contact Information

Please contact us by post or email if you have any questions about this Notice. Our contact details are shown below.

Title:
DPO (Legal & Compliance)

Address:
8668 John Hickman Parkway
Suite 1004
Frisco, Texas, USA – 75034

Email address:
dataprotection@MassMetric.com

If you would like this Notice in another format (for example: audio, large print, braille) please get in touch with us.

Version Control

Document Control	
Title	MassMetric Privacy Policy
Version	1.0
Date Issued	02-01-2025
Status	Sent for Approved
Document Owner	Legal
Author	Bijal Joshi
Author Title	Senior Manager Legal
Approver	Adithya Raj
Approver Title	CTO
Document Revision History	Initial Document Created
Review Due	Annual – January 2025