General Data Privacy Protection (GDPR) and California Privacy Act (CCPA) Mission Statement

1. Introduction

The EU General Data Protection Regulation ("**GDPR**") came into force on 25 May 2018. The Regulation aims to standardize data protection laws and processing across the EU, giving people greater rights to access and control their personal information.

In addition, you are probably already familiar with the California Consumer Privacy Act (''**CCPA'')**, which requires covered businesses (like most of our customers) to provide California residents substantially increased notice, access and control of their personal information.

For an overview of **GDPR** and **CCPA**, please see the following resources:

CCPA Fact Sheet

United Kingdom's Information Commissioners Office

The intent of this privacy brief is to provide an update regarding Navisite's current posture on certain aspects of the privacy laws as they apply to Navisite and the services we provide to you.

2. Our Commitment

Navisite is committed to conducting its business in accordance with applicable data privacy laws and regulations and in line with the highest standard of ethical conduct to ensure protection of individuals' and customers' information. Data **Confidentiality**, **Integrity** and **Availability** are our founding values.

We have always had a robust and effective data protection program in place, which complies with existing laws and abides by the data protection principles. To that end, we have updated and expanded our program to meet the demands of **GDPR** and **CCPA**.

3. Our Mission

Navisite's compliance and privacy mission is to establish a worldwide baseline standard for processing and protecting Personal Data by all Navisite Entities.

Navisite (as a processor/service provider) believes that a strong partnership with our clients (as controllers/"businesses") is an important part of the compliance relationship process. Navisite believes in being transparent with our clients as to our information security and data privacy practices.

Since Navisite is not a public authority or body, we do not collect special category data, which includes:

- Data related to racial or ethnic origin,
- Data related to political opinions,
- Data related to religious or philosophical beliefs,
- Data related to trade union membership,
- Genetic data,

- Biometric data (where used for identification purposes),
- Data concerning health,
- Data concerning a person's sex life, and
- Data concerning a person's sexual orientation.

4. How We Prepared for GDPR and CCPA

Navisite already has a consistent level of data protection and security across our organization. To meet GDPR and CCPA, we have introduced measures to ensure compliance:

- **Information Audit:** We have carried out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed, and if and to whom it is disclosed.
- **Documented Policies and Procedures:** We have revised data protection policies and procedures to meet the requirements and standards for GDPR and CCPA.
- **Privacy Policy/Notice:** We have revised our Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to, and what safeguarding measures are in place to protect their information.
- **Obtaining Consent:** We have reviewed our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, and why and how we use it. We have also provided clear, defined ways for them to consent to us how we process their information.
- **Direct Marketing:** We have revised the wording and processes for direct marketing, including adding clear opt-in mechanisms for marketing subscriptions, a clear notice and method for opting out, and unsubscribe features on all subsequent marketing materials.
- **Data Protection Impact Assessments (DPIA):** Where we process personal information that is considered high risk, we have developed stringent procedures for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity, and implement mitigating measures to reduce the risk posed to the data subject(s).
- **Processor Agreements**: Where we use any third-party to process personal information on our behalf (i.e., Payroll, Recruitment, Hosting, etc.), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they meet and understand their/our GDPR obligations.

5. Information Security and Technical Measures

Navisite's compliance program follows a process approach to ensure we demonstrate compliance with regulation and provide our customers assurances in relation to how we handle their personal data.

Navisite is in the process of building its information security (ISO/IEC 27002) and risk management (ISO/IEC 31000) frameworks to protect personal information from unauthorized access, alteration, disclosure or destruction.

6. Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information via **our website** of an individual's right to access any personal information that Navisite processes about them and to request information about:

- What personal data we hold about them.
- The purposes of the processing.
- The categories of personal data concerned.
- The recipients to whom the personal data has/will be disclosed.
- How long we intend to store their personal data.
- If we did not collect the data directly from them, information about the source.
- The right to have incomplete or inaccurate data about them corrected or completed, and the process for requesting this.
- The right to request the erasure of personal data (*where applicable*) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use.
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances.

7. Roles and Responsibilities

Navisite has a designated data compliance team to develop and implement our roadmap for complying with the data protection regulation. The team is responsible for promoting awareness of the GDPR/data privacy law across the organization; assessing our compliance; identifying any gap areas; and implementing the new policies, procedures and measures.

Navisite also understands that continuous employee education is key to the continued compliance of the GDPR and has involved our employees in our preparation plans.

If you have any questions about our GDPR/data privacy compliance policies, please contact: Privacy@Navisite.com.

8. Removing or Updating Your Information, or Changing Your Preferences

Please contact your Navisite customer success representative, or the Navisite data privacy team at the address or email below, if you:

- Would like your personal data removed.
- Prefer not to receive information from us.

- Have questions regarding our Privacy Policy, the accuracy of your personal information or the use of the information collected.

You can contact us by mail or email.

Address:
Navisite
400 Minuteman Road, Andover, MA 01810
Email: Privacy@Navisite.com