EUROPEAN UNION'S
GENERAL DATA PROTECTION REGULATION
FREQUENTLY ASKED QUESTIONS

On May 25, 2018, the European Union's General Data Protection Regulation (Regulation 2016/679) ("GDPR") went into effect. The GDPR is a regulation that requires entities, both within the European Union and outside of the European Union, to take certain proactive measures to ensure an adequate level of protection for personal data. These FAQs are intended to provide you with an overview of the GDPR's requirements and NAMSA's compliance with this regulation. If you have any additional questions regarding the GDPR, NAMSA's compliance with the GDPR and any other applicable data protection laws, please contact NAMSA at privacy@namsa.com.

1. **WHAT IS PERSONAL DATA?** – Personal data means any information relating to an identified or identifiable natural person (i.e., the data subject) that can be used to directly or indirectly to identify a natural person (Article 4(1)). Examples of personal data outlined by the GDPR include a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2. **DOES THE GDPR APPLY TO ANNOYMIZED/DE-IDENTIFIED DATA?** – The GDPR recognizes the ability to process personal data in a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information (Article 4(5)). Personal data that has undergone appropriate pseudonymization does not fall under the requirements of the GDPR. (Recital 26).

3. **WHO ARE CONTROLLERS, PROCESSORS AND SUB-PROCESSORS?** – There are two key roles under the GDPR: controllers and processors. Data controllers are entities that determine the purposes and means of the processing of personal data (Article 4(7)). The GDPR recognizes that there can be "joint controllers" where two or more controllers jointly determine the purposes and means of processing data (Article 26(1)). A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Article 4(8)). An entity who processes data on behalf of the processor is considered a sub-processor.

The GDPR requires that a controller ensure that any processor that processes personal data comply with the GDPR. Further, a controller and a processor must enter into an agreement that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller (Article 28(3)).

NAMSA's DPO is Jacqueline Torfin, Vice President, Global Quality Assurance and Regulatory Compliance. Contact information is privacy@namsa.com.

4. **WHAT IS A DATA PROTECTION OFFICER?** – In certain instances, the GDPR requires that a controller or processor designated a Data Protection Officer ("DPO") to manage that entity's data protection and facilitate compliance with the GDPR. The DPO is charged with overseeing activities carried out by the controller, processor, and any other entity that processes personal data. The DPO is the point of contact for supervisory authorities and data subjects for inquires related to the GDPR and the entity's compliance.

5. **WHAT ARE THE DATA SUBJECT RIGHTS UNDER THE GDPR?** – The GDPR includes many rights associated with personal data, including the right of access by the data subject (Article 15); the right to rectification (Article 16); the right to erasure ('right to be forgotten') (Article 17); the right to restriction of processing (Article 18); the right to data portability (Article 20); the right to object (Article 21); and the right not to be subject to a decision based solely on automated processing (Article 22). Controllers are required to proactively provide information related to data processing to data subjects in a concise, transparent, clear, and easily accessible form (Article 12(1)). If a data subject submits a request related to any of these rights, a controller must respond to that request within one month (Article 12(3)).

EUROPEAN UNION'S
GENERAL DATA PROTECTION REGULATION
FREQUENTLY ASKED QUESTIONS

6. **WHAT DOES GDPR MEAN BY "DATA PROTECTION BY DESIGN AND BY DEFAULT"?** – Data protection by design means incorporating privacy features and functionalities into the design of products and services to ensure the minimum amount of personal data is collected. Data protection by default means that entities implement appropriate measures to mitigate privacy risks at the time of collection of personal data and through the personal data's life cycle with the entity.

7. **HOW DOES NAMSA COMPLY WITH THE GDPR?** – NAMSA is committed to ensuring that adequate safeguards and data protection principles are used to ensure that any personal data in its custody is processed in an appropriate and compliant manner. NAMSA has designated a DPO to facilitate on-going compliance with the GDPR and to address any concerns that may arise regarding data protection generally. Considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons related to their personal data, NAMSA implements appropriate technical and organizational measures to ensure a level of security appropriate to protect personal data. To comply with the GDPR, NAMSA has developed internal data management processes to address data subject rights, data security, and data supply-chain management and expects its business partners to implement similar measures related to data protection.