SUPPLEMENTAL DATA PROCESSING INSTRUCTIONS REGARDING COMPLIANCE WITH APPLICABLE DATA PROTECTION LAWS ("Accenture's notice")

At Accenture, meeting the highest ethical standards is always of paramount importance. We treat privacy as a fundamental right for individuals and therefore take the protection of the personal data we handle internally and on behalf of clients very seriously. Following the publication of the European General Data Protection Regulation (GDPR) in 2016, which applies to processing of personal data of individuals in the EU, regardless of where it is processed or stored, Accenture built on an already strong privacy core to raise our commitment to privacy and data protection to new levels. As part of our robust privacy program, we continue to regularly monitor developments in privacy regulations globally and implement new requirements across all geographies as a consistent, global standard to address client and business needs.

As new consumer protection laws have developed, such as the California Consumer Privacy Act (CCPA) in the U.S., Accenture continues to analyze requirements and plan for the implementation of such laws as applicable to Accenture's business and services. As a Service Provider to Accenture, you have an important responsibility to protect the privacy and security of the information we or our clients share with you ("**You"**).

YOUR COMPLIANCE WITH THE CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")

As You may know, the California Consumer Privacy Act **("CCPA")** will come into effect **on January 1, 2020**. You and Accenture entered into agreements under which personal information is accessed, held or otherwise processed by You as part of your provision of goods, services or technology to Accenture and/or Accenture's clients ("**Agreements**"). Under CCPA You are acting as a **Service Provider** and because of that, we want to remind You of your legal and contractual obligations to Accenture with respect to personal information that, You may collect, retain, use, disclose or otherwise process as part of your relationship with Accenture.

Accenture relies on You to comply with all applicable legal obligations under laws and regulations that mandate the protection of personal information**.** Accenture engages only with Service Providers that implement appropriate technical and organizational security measures to protect personal information in compliance with applicable privacy laws. We expect that as part of these commitments, You will comply with Accenture's Notice.

As a Service Provider to Accenture, You may only process, use, retain the personal information of Accenture or Accenture's clients for the purpose to perform the contracted services, in particularly you cannot sell, use, retain or make available such personal information for any other purposes. On request, You must assist us without undue delay in ensuring that requests from and the legal rights of individuals to whom Accenture personal information relates are appropriately addressed, including access or delete personal Information.

By continuing your engagement with Accenture, You are certifying that You understand your above-mentioned contractual obligations and restrictions and will comply with them. These requirements must be flowed down to any sub-contractors that provide services on your behalf for Accenture or Accenture's Clients.

Additional information regarding your privacy obligations and your agreement(s) can be found in the Frequently Asked Questions (FAQs).

If You have any questions regarding this **Accenture Notice**, please contact your respective Accenture contact. We thank you for being our trusted Service Provider.

YOUR COMPLIANCE WITH THE GENERAL DATA PROTECTION REGULATION ("GDPR")

The European Union has adopted Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation" or "GDPR"), with an effective date of 25 May 2018.
Accenture's suppliers ("Provider") and Accenture enter into agreements under which personal data is accessed, held or otherwise processed by Provider as part of its provision of goods, services or technology to Accenture and/or Accenture's clients ("Agreements").
Accenture relies on Provider to comply with all applicable legal obligations under laws and regulations that mandate the protection of personal data, which include those under the GDPR.
The GDPR requires, among other things, that Accenture engages only with suppliers that implement appropriate technical and organisational security measures to protect personal data in compliance with the regulation. To comply with the GDPR, Accenture is required to have certain GDPR-compliant terms included in our agreements where personal data is being processed. For this reason, Accenture asks its suppliers to sign Accenture's Data Privacy Amendment through Accenture's Supplier Management Portal.
Nevertheless, GDPR is an existing legal obligation on both Accenture and Provider, as part of the general obligation on both parties to comply with applicable laws. Accenture also may issue data processing instructions to Provider. Therefore, for both of these reasons, we expect Provider to comply with the following GDPR requirements and data processing instructions, specifically:

- Provider will only process personal data on Accenture's written instructions or in accordance with applicable laws;
- Provider will not retain personal data for longer than is necessary;
- Provider will not transfer personal data outside of the jurisdictions to which the parties have agreed, without Accenture's prior written consent;
- Provider will impose a duty of confidentiality on its staff with access to personal data;
- Provider will require that any sub-processor must comply, under a written agreement, with the same standards as Provider to meet the requirements of the GDPR, and Provider will remain fully liable for the sub-processor's performance;
- Provider will, to the extent possible, assist and cooperate with Accenture in responding to requests made by data subjects exercising their rights under the GDPR, including rights of access, rectification, correction, erasure and portability;
- Provider will implement technical and organizational security measures, including encryption of personal information, implementing business continuity and disaster recovery plans, and regularly testing and evaluating security measures;
- Provider will assist Accenture with carrying out privacy and data protection impact assessments and related consultations with supervisory authorities;
- Provider will securely delete (or return at Accenture's request) all personal data upon expiration or termination of an individual Agreement;
- Provider will provide information to Accenture and supervisory authorities reasonably required to demonstrate compliance with the GDPR and assist with audits of Provider's data processing activities to verify compliance with the GDPR;
- When responding to audits or other information requests, Provider will notify Accenture immediately in writing if, in Provider´s opinion, Accenture´s instructions breach the GDPR;
- Provider will promptly notify Accenture in writing whenever Provider knows or reasonably suspects a security breach has occurred, and investigate and remediate the breach, including cooperating with Accenture's investigation and remediation efforts.

By continuing to provide goods, services or technology to Accenture under the Agreements, Provider agrees to comply with GDPR requirements, including those requirements outlined above.