SUPPLEMENTAL DATA PROCESSING INSTRUCTIONS AND STATEMENT REGARDING 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.