ACCENTURE PRIVACY STATEMENT FOR MANAGED DETECTION & RESPONSE SERVICES

This Privacy Statement ("**Privacy Statement**") is effective as of May 24, 2021 and is available for your review in the following languages:

SPANISH | PORTUGUESE | ITALIAN | JAPANESE

In the event of any conflict between the English version of this Privacy Statement and a translated version of this Privacy Statement, the English version shall prevail.

Please note that this Privacy Statement will regularly be updated to reflect any changes to the interactions Accenture has with you and the MDR Services and details the nature of personal data Accenture collects and processes, how Accenture processes such personal data and for what purposes or any changes in applicable laws.

Accenture provides certain Managed Detection & Response Services ("**MDR Services**") in connection with an agreement between Accenture and an entity, organization, or business that you are affiliated or otherwise associated with, such as your employer ("**Your Organization**") that governs the use of the MDR Services ("**Terms of Use**). Accordingly, this Privacy Statement applies to the interactions Accenture has with you and the MDR Services and details the nature of personal data Accenture collects and processes, how Accenture processes such personal data and for what purposes.

Your Organization has acquired the MDR Services for its organizational purposes. Accordingly, your access to the MDR Services is managed according to the Terms of Use. Your Organization may also have access to and process your personal data, including any interaction with the data, diagnostic data, and the contents of your communications and any files associated with your use of the MDR Services, along with any accounts you sign in to which are acquired by Your Organization for its organization's purposes. To the extent Your Organization processes your personal data, you should direct all privacy inquiries, including any request to access your data protection rights to Your Organization's administrator. To the extent Accenture processes your personal data in connection with the MDR Services, you can refer to this Privacy Statement.

The MDR Services extend Your Organization's internal security operations program by monitoring Your Organization's IT environment on a 24x7 basis and applying global threat intelligence to detect advanced attacks.

To the extent that you use the MDR Services in connection with the Terms of Use, Accenture may provide information regarding your use of the MDR Services to Your Organization and other parties such as third-party service providers and public authorities as required by applicable law. Any third-party service providers and professional advisors to whom your personal data is disclosed, are required and expected to protect the confidentiality and security of your personal data and may only use your personal data in compliance with applicable data protection laws.

For the MDR Services, Accenture collects and processes the following categories of personal data:

PERSONAL DATA ELEMENTS COLLECTED AND PROCESSED

CATEGORY OF PERSONAL INFORMATION	TYPES OF PERSONAL INFORMATION CAPTURED
Log on, system and application access data and Internet and electronic network activity information.	Where you are provided with access to the MDR Services, including Accenture systems such as the MDR Services Portal, Accenture may collect information required to access such Accenture systems and applications such as System ID, LAN ID, e-mail account, instant messaging account, mainframe ID, system passwords, and internet or other electronic network activity information, including access logs, activity logs, and electronic content produced using Accenture systems.
Individual Identifiers and Characteristics (Name, User ID).	Your Organization's employees, contractors, clients, suppliers, and other business contracts, as well as other persons interacting electronically in or with Your Organization's networks.
Location data (device and network), IP Address.	Your Organization's employees, contractors, clients, suppliers, other business contacts, as well as other persons interacting electronically in or with Your Organization's networks.

Contact Information (business email address, corporate phone number).	Your Organization's employees and contractors, as well as potentially customers, suppliers, other business contacts and other persons interacting electronically in or with Your Organization's networks.

PERSONAL DATA RETENTION SCHEDULE. For the duration of the contractual relations between Accenture and Your Organization for MDR Services, personal data is retained by Accenture as described in the MDR Service description published by Accenture at https://www.accenture.com/us-en/support/security/legal-terms-managed-security ("**MDR Service Description**"). After the expiration or termination of the contractual relationship between Accenture and Your Organization for MDR Services, personal data is decommissioned except where its retention is required by applicable law, in which case personal data covered by such requirement will be further retained for the legally prescribed period.

DISCLOSURE AND INTERNATIONAL TRANSFER OF PERSONAL DATA. Accenture will send personal data to internal recipients, affiliated Accenture entities and external recipients (third party sub-processors), in the facilitation or provision of the MDR Services.

THIRD-PARTY SUB-PROCESSORS. Accenture utilizes several third-party sub-processors in the provision of the MDR Services. A list of such third-party sub-processors is available upon request from your Service Delivery Lead.

INTERNATIONAL TRANSFERS OF PERSONAL DATA. You are advised that Accenture and its affiliated entities will transfer personal data to locations outside of the European Economic Area and potentially outside of the country from which you are accessing the MDR Services, including to external recipients as described above. Any transfers of personal data from within the European Economic Area (EEA) to third parties outside the EEA will be based on an adequacy decision or are governed by the standard contractual clauses (a copy of which can be obtained through the contact information included below). Any other non-EEA related transfers of your personal data will take place in accordance with the appropriate international data transfer mechanisms and standards.

Personal data will be transferred to or accessed from the U.S.A., UK, Japan, Singapore, India, Australia, and such other countries as are determined by the MDR Services (including for storage, backup and archiving). For a comprehensive list please contact your Service Delivery Lead.

EXERCISE OF DATA SUBJECT RIGHTS. Your Organization's assigned administrators for MDR Services can create, edit or delete the personal information you have submitted. An Administrator can also contact the Accenture MDR Services team to create, edit or delete your contact information. Personal information gathered from you in the course of provisioning, setup and/or confirmation of the MDR Services will not be used for commercial resale purposes. Please contact your MDR Administrator or Organization if you wish to exercise these rights.

COOKIES. In addition to the information set out above, the **MDR COOKIES STATEMENT** describes how Accenture uses cookies based on your access to the MDR Services Portal. Cookies are text files containing small amounts of information which are downloaded to your computer or mobile device when you visit the MDR Services Portal and allow the MDR Services Portal to recognize your computer or mobile device. To exercise your choices for the MDR Services Portal, please visit the MDR Services Portal and adjust your cookie settings via the cookie consent manager or cookie settings button.

For complete details and additional information as to how Accenture collects, processes and secures personal data, and Accenture's commitment to protecting privacy, please see **ACCENTURE'S PRIVACY STATEMENT**.