



ACCENTURE PRIVACY STATEMENT FOR MANAGED EXTENDED DETECTION & RESPONSE SERVICES

This Privacy Statement ("**Privacy Statement**") is effective as of **January 1, 2022** 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.

WHY ARE YOU INTERACTING WITH ACCENTURE IN THE CONTEXT OF MxDR SERVICES. Accenture provides certain Managed Extended Detection & Response Services ("**MxDR 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 by Your Organization of the MxDR Services ("**Terms of Use**").

Accordingly, this Privacy Statement applies to your interactions with Accenture through your use and access to the MxDR Services (including, your use and access to Accenture's web portal through which you may, on behalf of Your Organization, access and use the MxDR Services ("**MxDR Portal**") and details the personal data Accenture collects and processes, how Accenture processes such personal data and for what purposes. For the purposes of this Privacy Statement, "**Accenture**" shall mean the Accenture entity that has entered into the Terms of Use with Your Organization. For clarification, any Accenture entity located outside the European Union will for the purposes of compliance with data privacy laws be represented by Accenture PLC.

WHICH OF YOUR PERSONAL DATA PROCESSED IN THE CONTEXT OF MxDR SERVICES IS CONTROLLED BY YOUR ORGANIZATION. Certain of your personal data, that is processed by Accenture in the context of the MxDR Services, has been provided to Accenture by Your Organization, when designating you as authorized user of the MxDR Portal. This personal data includes your name, e-mail address and contact details, as necessary to create/manage your user account for your use and access to the MxDR Portal. In addition, Accenture will process your personal data that may be included in security data (e.g. log data) that Accenture processes for the purposes of delivering the MxDR Services to Your Organization, as well as your personal data that is shared with Accenture during support sessions. Accenture processes such personal data upon instruction and on behalf of Your Organization in accordance with the Terms of Use, where a detailed list of all such personal data is provided.

If you have any doubts or queries relating to your personal data as detailed above, you should refer to Your Organization's privacy policy and direct all privacy inquiries, including any request to exercise your data privacy rights, to Your Organization's administrator. When contacted in this respect by you, Accenture, as processor, will refer any queries to Your Organization, in its capacity as controller of your personal data.

WHICH OF YOUR PERSONAL DATA PROCESSED IN THE CONTEXT OF MxDR SERVICES IS CONTROLLED BY ACCENTURE. When you interact with Accenture on behalf of Your Organization, through your use and access to the MxDR Services (including your use and access to the MxDR Portal or any other communication tools), Accenture will collect and process your personal data, as detailed below, for Accenture's own business purposes, including for contract management, payment processing, service offering, and business development purposes (as applicable). In respect to such processing activities, Accenture will act as a controller and this Privacy Statement shall apply to such processing activities by Accenture.

TYPE OF PERSONAL DATA PROCESSED	DATA SUBJECTS (categories)	PURPOSE OF THE PROCESSING	LEGAL BASIS
Account data • Title • Name • Business E-mail • Address • Telephone Number • Business Address.	• Individual(s) appointed by Your Organization to represent Your Organization in and during the contractual relationship and to otherwise interact with Accenture.	• Entering into contract for the provision of the applicable MxDR Service. • Communication with Your Organization in the provision of the applicable MxDR Service. • Communication with Your Organization in the event of complaints. • Invoicing and receiving payment for the applicable MxDR Service. • Exploring future contracting opportunities. • Performing and analyzing surveys and feedback. • Exercising or defending Accenture rights in the context of legal claims/disputes with Your Organization.	• Legitimate interest of both Accenture and Your Organization for having the MxDR Service contract in place properly performed. • Legitimate interest of Accenture for ensuring the proper functioning of its business operations and exercise its legal rights in case of claims/disputes with clients.



<p>Your interaction with the MxDR Portal</p> <ul style="list-style-type: none"> • Personal data contained in any form of communications sent/received through the MxDR Portal, search data and history, caches of viewed content, language preference. • Personal data collected through technical cookies (i.e., IP Address, Device ID, browser used, logs file). 	<ul style="list-style-type: none"> • Individual(s) appointed by Your Organization to represent it in and during the contractual relationship and to otherwise interact with Accenture. 	<ul style="list-style-type: none"> • Performing the contract for the provision of the applicable MxDR Service. • Enhancing the applicable MxDR Service. • Ensuring the operation and security of the MxDR Portal. • Exercising or defending Accenture rights in the context of legal claims/disputes with Your Organization. 	<ul style="list-style-type: none"> • Legitimate interest of both Accenture and Your Organization for having the MxDR Service contract in place properly performed. • Legitimate interest of Accenture for ensuring the proper functioning of its business operations, enhancing Accenture products and services, and exercise its legal rights in case of claims/disputes with clients.
<p>Security Data & Customer Care Data</p> <ul style="list-style-type: none"> • Personal data contained in Security Events and Activity Logs e.g., IP Address, Email Address, MAC Address, Host, Usernames, Device IDs and similar Unique Identifiers, Event ID, Process ID, Machine ID, WAP and/or Web Logs Files, Browsing Logs, Session Logs, Location Data (device and network locale). • Personal data contained in requests for support through Chat, Email, Voicemail, SMS/MMS (personal data may include Security Data processed in connection with the provision of applicable MxDR Service, as may be required for Your Organization to detail its request and for Accenture to action such request for support e.g. location data, network activity data, authentication data). 	<ul style="list-style-type: none"> • Your Organization's employees, contractors, clients, suppliers, as well as other persons interacting electronically in or with Your Organization's networks. 	<ul style="list-style-type: none"> • Developing threat intelligence activities. • Development and enhancement of any Accenture security products and services. • Gathering and compiling security event data to look at trends, and real or potential security threats. <p>NOTE: The results of such processing will be compiled or combined in an aggregated, and de-identified manner that will not in any way reveal the personal data as being attributable to the particular individual(s).</p>	<ul style="list-style-type: none"> • Legitimate interest of Accenture for ensuring the proper functioning of its business operations and enhancing Accenture security products and services

In respect to Accenture legitimate interests mentioned in the table above, Accenture is of the opinion that its legitimate interests are not overridden by your interests, rights or freedoms, given: (i) the transparency that Accenture provides on its processing activities; (ii) Accenture's privacy by design approach; (iii) Accenture's regular privacy reviews; and (iv) the rights you have in relation to Accenture's processing activities. If you wish to obtain further information on this balancing test approach, please contact [ACCENTURE'S DATA PRIVACY OFFICER](#).

DISCLOSURE OF YOUR PERSONAL DATA. When processing your personal data for the purposes listed in the table above, Accenture may disclose your personal data to internal and third-party recipients, that will be appointed as Accenture's processors as necessary according to applicable data privacy laws. For example, these recipients may include professional advisors and third-party service providers that provide services to Accenture, including billing, payment processing, customer service, email deployment, security and performance monitoring, maintaining or servicing accounts, processing or fulfilling orders and transactions, verifying customer information, research, data hosting and auditing.

Your personal data might also be shared with public and governmental authorities as required by applicable law. Furthermore, since you will be interacting with Accenture, through your use and access to the MxDR Services (including through your use and access to the MxDR Portal), on behalf of Your Organization, Accenture may provide your personal data to Your Organization, if so requested or when necessary pursuant to the Terms of Use.

Additionally, as a global organization with offices and operations throughout the world, your personal data may be transferred or be accessible internationally throughout Accenture's global business and between its entities and affiliates, also in connection with Accenture's operation of its business, including any (potential) corporate or commercial transaction (such as the sale of a website, a merger, consolidation, asset sale, initial public offering, or in the unlikely event of a bankruptcy).



Before disclosing your personal data to any recipients, Accenture shall take the necessary steps to ensure that your personal data will be given adequate protection as required by applicable data privacy laws and Accenture's internal policies.

INTERNATIONAL TRANSFERS OF YOUR PERSONAL DATA. Any transfer of your personal data from within the European Economic Area ("EEA") to third party recipients outside the EEA will be based on an adequacy decision by the EU Commission or be governed by the applicable standard contractual clauses (a copy of which can be obtained through Accenture Service Delivery Lead). Any transfers occurring throughout Accenture's global business will take place in accordance with the applicable data privacy laws and Accenture's [BINDING CORPORATE RULES FOR CONTROLLERS](#). Any other non-EEA personal data-related transfer will take place in accordance with the appropriate international data transfer mechanisms and standards.

PERSONAL DATA RETENTION SCHEDULE. Your personal data will be retained for the duration of our contractual relationship with Your Organization in respect to the MxDR Services and, after its expiration or termination, for as long as needed in order to comply with our global legal and contractual obligations. Accenture maintains specific records management and retention policies and procedures, so that personal data is deleted after a reasonable time according to the retention criteria indicated above. In case of disputes or claims, Accenture may retain your personal data as necessary for exercising or defending Accenture's rights until the resolution of the dispute/claim.

EXERCISE OF YOUR RIGHTS AS DATA SUBJECT. You are entitled (in the circumstances and under the conditions, and subject to the exceptions, set out in applicable data privacy laws) to: **(i)** request **access** to your personal data Accenture processes: this right entitles you to know whether Accenture holds personal data about you and, if it does, to obtain information on and a copy of that personal data; **(ii)** request a **rectification** of your personal data: this right entitles you to have your personal data be corrected if it is inaccurate or incomplete; **(iii)** **object** to the processing of your personal data: this right entitles you to request that Accenture no longer processes your personal data; **(iv)** request the **erasure** of your personal data: this right entitles you to request the erasure of your personal data, including where such personal data would no longer be necessary to achieve the purposes; **(v)** request the **restriction of the processing** of your personal data: this right entitles you to request that Accenture only processes your personal data in limited circumstances, including with your consent; **(vi)** request **portability** of your personal data: this right entitles you to receive a copy (in a structured, commonly used and machine-readable format) of personal data that you have provided to Accenture, or request Accenture to transmit such personal data to another data controller.

To the extent the processing of your personal data falls in scope of Accenture's [BINDING CORPORATE RULES FOR CONTROLLERS](#), you may also want to review your rights under such Binding Corporate Rules for Controllers.

If, despite Accenture's commitment and efforts to protect your personal data, you believe that your data privacy rights have been violated, Accenture encourages and welcomes individuals to come to Accenture first to seek resolution of any complaint. You have the right at all times to register a complaint directly with the relevant supervisory authority or to make a claim against Accenture with a competent court (either in the country where you live, the country where you work or the country where you deem that data privacy law has been infringed). [CONTACT US](#) to exercise any of your rights.

ADDITIONAL INFORMATION. For complete details and additional information as to how Accenture processes and secures your personal data and Accenture's commitment to protecting your privacy, review Accenture's [GLOBAL PRIVACY STATEMENT](#).

COOKIES. In addition to the information set out above, please see the [MxDR COOKIES STATEMENT](#) that describes how Accenture uses cookies based on your use and access to the MxDR Portal.

UPDATES TO THIS PRIVACY STATEMENT. Please note that this Privacy Statement will regularly be updated to reflect any changes to the interactions Accenture has with you and the MxDR 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.