Effective date: 5/7/2022
Last updated date: 11/1/2023

ADP US Employee Electronic Monitoring Notice

This US Employee Monitoring Notice ("Notice") explains how Automatic Data Processing, Inc. ("ADP") monitors the use of ADP electronic communication systems. This Notice supplements information provided in the GSO Secure Communications Standard.

1. Monitoring of Electronic Communication Systems

ADP provides electronic communication systems to facilitate ADP's business. Any and all telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage by an employee by any electronic device or system, including but not limited to the use of a computer, telephone, wire, radio or electromagnetic, photoelectronic or photo-optical systems may be subject to monitoring at any and all times and by any lawful means.

ADP may monitor its electronic communication systems and all messages transmitted through or stored on these systems to determine compliance with its policies, conduct internal investigations regarding misconduct or any other business issue, investigate a security event or incident, answer a lawful subpoena or court order, exercise or defend a legal claim, respond to a client need, maintain business continuity, locate information, or for any other business purpose, consistent with applicable law.

2. Data Collected from ADP Electronic Communication Systems

In the course of the monitoring described above, ADP may collect information about personnel, including the information described below. Although this list is intended to inform you about the types of monitoring that ADP performs, it may not be comprehensive, and ADP may perform additional similar types of monitoring that are not specifically addressed below, as permitted by applicable law.

- **Card/Key Entry Access** – ADP may collect information regarding personnel use of key cards or other physical security devices to provide access to ADP facilities, elevators, floors and areas with keyed access.

- **Continuous Video Surveillance** – such surveillance is used throughout ADP offices, including at main entry/exit points, hallways, loading docks, parking lots and decks, and other workplace sensitive areas (but not in private locations, such as individual offices or restrooms).

- **Telephone Use and Voicemail** – ADP may collect information regarding inbound and outbound calls made by personnel and their duration. Contents of voicemail may be accessed and reviewed by authorized ADP personnel for the purposed described above. Certain types of calls may be recorded or monitored in real time, subject to additional notices provided to you for the applicable situations (for example, customer service

calls or internal training calls). **Email** – Authorized ADP Personnel may access and review your emails for the purposes described above.

- **Use of Documents and Data** – ADP may review records of access to and actions taken on documents, files and other data on network shares, databases, applications, ADP cloud resources, collaboration tools, or other repositories.

- **Internet Use** – ADP may review sites visited, time and duration of visited, and volume of data transferred to or from the site, and specific files transferred.

- **Network and Remote Access** – ADP may collect and review date, time, and location of network login, count and duration of remote connections, and access to network resources.

- **Downloads** – ADP may collect and review the details of files and downloads of data from network resources to local devices.

- **Data Loss Prevention (DLP)** – To safeguard the confidentiality and integrity of ADP and client information, ADP uses a DLP solution that monitors and potentially block specific activities involving certain types of sensitive data (e.g., Social Security numbers, W-2 Employer Identification Numbers, credit or debit card numbers, or bank account numbers) on ADP-issued systems, including (a) saving such data to portable media, (b) printing documents containing such data, (c) emailing such data to recipients outside ADP, and (d) transmitting such data outside ADP's systems and networks.

3. Questions

If you have any questions about this Notice, please contact GHRSS at 1-877-237-4711.