SASB Disclosure

Our responses to the SASB disclosures were written in an attempt to include as much of the requested information as possible. As this report reflects our first step in our SASB journey, only partial information is available at this time in some instances. We look forward to reporting more comprehensively under this framework in the years ahead.

Topic	Accounting Metric	Disclosure	Code
Environmental Footprint of Hardware and Infrastructure	(1) Total energy consumed, (2) percentage grid electricity, (3) Percentage renewable	Please see ADP's 2020 ESG Metrics Sheet, Energy and Greenhouse Gas Reductions and Data Centers sections of this report.	TC-SI-130a.1
Data Privacy and Freedom of Expression	Description of policies and practices relating to behavioral advertising and user privacy	The collection, storage, hosting, transfer, processing, disclosure, use, security, retention and destruction of personal information required to provide our services is done in compliance with federal, state and foreign privacy, data protection and cyber security laws. We are committed to respecting our users' choices regarding their personal data. Only in rare circumstances, as described in our BCR, will we process user data for a legitimate secondary purpose. We do not transfer personal data to third-party providers other than to perform ADP services, after they have contractually agreed to follow our privacy principles. Further our products do not target children. ADP does not have a unique retention schedule based on data or data types due to their varied nature across business units. To learn more, please see our Global Records Information Management Program. For more information on the scope and implementation of our practices related to user privacy, please see ADP's Privacy page. For more information on our Binding Corporate Rules (BCR) regarding the collection, retention, protection and usage of personal data, please see ADP's Global Privacy Policy.	TC-SI-220a.1
	Number of users whose information is used for secondary purposes	ADP does not currently track this information.	TC-SI-220a.2
	Total amount of monetary losses as a result of legal proceedings associated with user privacy	Please see ADP's 10-K and 10-Qs for a description of any material monetary losses as a result of legal proceedings associated with user privacy.	TC-SI-220a.3
	(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure	Please see our 10-K and 10-Qs for a description of any materials requests from law enforcement.	TC-SI-220a.4

SASB Disclosure

Topic	Accounting Metric	Disclosure	Code
Data Security	(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected	While ADP maintains and continually enhances its global security program, including extensive business, system, and network security controls and processes, issues that ADP characterizes as security incidents do occasionally occur. Such security incidents do not necessarily constitute security breaches as defined by law. ADP's policy requires the prompt reporting of all such security incidents, and appropriate investigation and evaluation to ensure that all incidents are addressed timely and effectively, and in accordance with ADP policy and applicable legal requirements. All issues to date have been limited in scope and have included, for example, hard copy or electronic misdeliveries of client information. Given today's threat landscape, all large organizations are targeted by cyber-attacks. ADP's security program is designed to prevent or detect such attempts via ADP's security intelligence platform, while leveraging partnerships with law enforcement and threat intelligence organizations to enhance our capabilities. ADP's incident response process is initiated during any identified attempt. Within ADP's global security program, comprehensive enterprisewide policies and procedures are in place for managing, tracking and reporting security incidents. ADP's security policies require logging of all actual security incidents reported to ADP by its associates, clients or other third parties. Once a security incident is reported, ADP's incident response process is designed to ensure that all incidents are addressed in a timely and effective manner and are in accordance with ADP security policies, procedures and legal requirements. When necessary, procedures for notifying clients without undue delay, as well as employees and all other parties who may be impacted by the incident, are initiated and appropriate remedial actions are taken. For more information please see our disclosure on Incident Management in our Data Security page.	TC-SI-230a.1
	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	ADP policy requires our management to promptly take appropriate actions and commit sufficient resources to reduce unacceptable loss exposures to acceptable levels. To meet this objective ADP has an operational risk management framework and has deployed supporting procedures and tools across the enterprise. ADP Operational Risk Management is responsible for maintaining the framework while integrating with Enterprise Risk Management for aggregation and escalation. The ADP Executive Committee provides operational risk governance through the Executive Security Council, which is chaired by the Chief Security Officer and includes the CEO, CFO, CIO, CHRO (Chief Human Resources Officer), and General Counsel. The ADP operational risk management framework is based on the following industry standards: • Overall Risk Process: Enterprise Risk Management–Integrated Framework (COSO-ERM); ISO 31000: 2009 Risk Management – Principles and Guidelines; The Risk IT Framework (ISACA); COBIT 5 for Risk (ISACA). • Risk Analysis Approach: The Open Group Risk Taxonomy Standard (O-RT); The Open Group Risk Analysis Standard (O-RA). We are focused on ensuring that we are safeguarding and protecting personal and business information and client funds, and we devote significant resources to maintain and regularly update our systems and processes. ADP's vendors must meet our data security and privacy standards. Our vendor assurance process enables ADP to assess our vendors prior to entering into a contract with them. Our vendors are contractually required to comply with ADP's privacy principles. For more information please see our Data Security page.	TC-SI-230a.2

SASB Disclosure

Recruiting & Managing a Global, Diverse & Skilled Workforce	Employee engagement as a percent	Please see the Training and Development on page 26 of this report.	TC-SI-330a.2
	Percentage of gender and racial/ethnic group representations for (1) management, (2) technical staff, and (3) all other employees	Please see the Diversity & Inclusion section on page 16 of this report.	TC-SI-330a.3
Managing System Risk	Number of (1) performance issues and (2) service disruptions; (3) total customer downtime	ADP serves over 810,000 clients in more than 140 countries through an array of products and services that meet our clients' unique human resource and compliance needs across the globe. While rare, there are times when our products may experience temporary, unplanned service disruptions due to unforeseen circumstances. Typically, these outages are limited to one targeted region, product or country and do not impact the majority of our clients.	TC-SI-550a.1
	Description of business continuity risks related to disruptions of operations	ADP is committed to keeping our services and operations running smoothly to provide our clients with the best service possible. It's our priority to identify and mitigate the technological, environmental, process and health risks that may interfere with the services we provide to our clients. For this reason, we have created an integrated framework that lays out our mitigation, preparedness, response and recovery process. For more information, please see our Business Resiliency Fact Sheet as well as the risks outlined in our 10-K and our proxy statement.	TC-SI-550a.2