

# SUSTAINABILITY ACCOUNTING STANDARDS BOARD (SASB) DISCLOSURE - CD PROJEKT S.A. 2024

## SOFTWARE & IT SERVICES

TOPIC	ACCOUNTING METRIC	CODE	DISCLOSURE
ENVIRONMENTAL FOOTPRINT OF HARDWARE INFRASTRUCTURE	1. Total energy consumed, 2. percentage grid electricity 3. percentage renewable	TC-SI-130a.1	1. 12 844 GJ 2. 60 % 3. 3 %
	1. Total water withdrawn 2. total water consumed, percentage of each in regions with High or Extremely High Baseline Water Stress	TC-SI-130a.2	1. 18 thousand m <sup>3</sup> 2. 18 thousand m <sup>3</sup> ; 0%
	Discussion of the integration of environmental considerations into strategic planning for data center needs	TC-SI-130a.3	Much of the service is provided from our own servers, located at CD PROJEKT's headquarters in Warsaw. Our computing resources are virtualized and/or containerized, thus ensuring a high resource utilization rate. In addition, some services are also implemented with the help of public cloud providers, including AWS, Google Cloud Platform. Cloud solutions are taken into account when planning new solutions. Public cloud providers completely or significantly use renewable energy. Servers in Warsaw are powered by electricity from the company's own photovoltaic panels and energy purchased for CD PROJEKT's complex in Warsaw. In 2024, CD PROJEKT signed an agreement to purchase electricity from 100% renewable sources, which powers the Warsaw campus from 01.01.2025.
DATA PRIVACY & FREEDOM OF EXPRESSION	Description of policies and practices relating to behavioral advertising and user privacy	TC-SI-220a.1	Personal data is processed in accordance with the internal Personal Data Protection Policy and the publicly available CD PROJEKT RED Privacy Policy. There is no dedicated policy relating specifically to behavioral advertising.
	Number of users whose information is used for secondary purposes	TC-SI-220a.2	We did not prepare a summary of data from this area during the reported period.
	Total amount of monetary losses as a result of legal proceedings associated with user privacy	TC-SI-220a.3	0 PLN – we did not incur such losses in the reported period
	1. Number of law enforcement requests for user information, 2. number of users whose information was requested, 3. percentage resulting in disclosure	TC-SI-220a.4	0 – no such requests regarding users of our services in the reported period
	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring	TC-SI-220a.5	W raportowanym okresie nie przygotowaliśmy zestawienia danych z tego obszaru.

TOPIC	ACCOUNTING METRIC	CODE	DISCLOSURE
DATA SECURITY	1. Number of data breaches, 2. percentage involving personally identifiable information (PII), 3. number of users affected	TC-SI-230a.1	During the reported period, we noted 1 case of sharing personal data of the Company's customers with an unauthorized person. The violation involved the personal data of 2 customers.
	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	TC-SI-230a.2	As part of the risk management process at CD PROJEKT S.A., operational risk of unavailability of IT infrastructure or services, including cyber security risk, was identified. The risk was analyzed in accordance with the Company's methodology. Risks and possible opportunities related to the management of this risk were identified and described. Action plans for various forms of risk materialization, which include a description of mitigation actions, are developed and successively improved. A description of the identified risks can be found in the <u>Management Board report on CD PROJEKT Group activities for 2024</u> . Cyber risk is the potential exposure to loss or damage resulting from the fact that data is processed in information or communication systems. Cyber risks go beyond data corruption, leakage or destruction and may also involve theft of intellectual property, loss of productivity or reputational damage. The consequences of a potential breach can range from weakened brand reputation and lost revenue to falling stock prices. These consequences also involve the costs of pursuing claims, prosecuting possible tortfeasors, implementing remedial or loss minimization measures, and possibly imposing financial penalties or compensation obligations on the Company.
RECRUITING & MANAGING A GLOBAL, DIVERSE & SKILLED WORKFORCE	4. Percentage of employees that are: 1. foreign nationals 2. located offshore	TC-SI-330a.1	1. 20% 2. 5%
	Employee engagement as a percentage	TC-SI-330a.2	78% – the score of the engagement survey conducted with the Culture Amp tool.
	Percentage of gender and racial/ethnic group representation for 1. management 2. technical staff 3. all other employees	TC-SI-330a.3	1. women: 27%, men: 73%; Poles: 85 %, foreigners: 15% 2. women: 22%, men: 78%; Poles: 75%, foreigners: 25% 3. women: 50%, men: 50%; Poles: 87%, foreigners: 13%

TOPIC	ACCOUNTING METRIC	CODE	DISCLOSURE
INTELLECTUAL PROPERTY PROTECTION & COMPETITIVE BEHAVIOR	Total amount of monetary losses as a result of legal proceedings associated with anti- competitive behavior regulations	TC-SI-520a.1	0 PLN – we did not incur such losses in the reported period
MANAGING SYSTEMIC RISKS FROM TECHNOLOGY DISRUPTIONS	Number of 1. performance issues 2. service disruptions 3. total customer downtime	TC-SI-550a.1	n/a – CD PROJEKT does not provide services to clients based on cloud solutions
	Description of business continuity risks related to disruptions of operations	TC-SI-550a.2	As part of the risk management process at CD PROJEKT S.A., operational risk of unavailability of IT infrastructure or services, including cyber security risk, was identified. The risk was analyzed in accordance with the Company's methodology. Risks and possible opportunities related to the management of this risk were identified and described. Action plans for various forms of risk materialization, which include a description of mitigation actions, are developed and successively improved. A description of the identified risks can be found in the <u>Management Board report on CD PROJEKT Group activities in 2024</u> . The identified risk relates to loss of access to IT infrastructure or business applications supporting critical business processes at CD PROJEKT as a result of an unforeseen event. This risk represents potential exposure to loss or damage resulting from an interruption in the availability of CD PROJEKT's ICT systems. The risk goes beyond physical or logical damage to infrastructure components or data processing systems and also includes loss of physical access to server rooms and other data processing locations.