

# **MSCI ESG Ratings Methodology: Privacy & Data Security Key Issue**

MSCI ESG Research LLC

October 2023

**Contents**

Introduction..... 3

Risks associated with this Key Issue..... 4

Privacy & Data Security Key Issue Score ..... 4

Privacy & Data Security Management Score..... 5

    Management Score category: Practices Score..... 5

    Controversies..... 7

Privacy & Data Security Exposure Score..... 7

    Business Exposure Score..... 8

        Business Segment Exposure Scores..... 9

    Geographic Exposure Score..... 10

        Geographic Segment Exposure Scores..... 11

    Company-Specific Exposure Score..... 12

    Data Sources..... 12

## Introduction

This document provides essential information on the components of the Privacy & Data Security Key Issue to enable users of ESG Ratings to understand how our outputs are determined. Privacy & Data Security is a Key Issue in the Social Pillar of the MSCI ESG Ratings model. Companies are evaluated on the amount of personal data they collect, their exposure to evolving or increasing privacy regulations, their vulnerability to potential data breaches, and their systems for protecting personal data.

For additional details on the MSCI ESG Ratings Model, refer to Section 2, Data, ratings and scores, of “ESG Ratings Methodology.”

**Exhibit 1: MSCI ESG Key Issue hierarchy**

3 Pillars	10 Themes	33 ESG Key Issues
Environmental	Climate Change	Carbon Emissions
		Climate Change Vulnerability
		Financing Environmental Impact
		Product Carbon Footprint
	Natural Capital	Biodiversity & Land Use
		Raw Material Sourcing
		Water Stress
	Pollution & Waste	Electronic Waste
		Packaging Material & Waste
		Toxic Emissions & Waste
	Environmental Opportunities	Opportunities in Clean Tech
		Opportunities in Green Building
		Opportunities in Renewable Energy
Social	Human Capital	Health & Safety
		Human Capital Development
		Labor Management
		Supply Chain Labor Standards
	Product Liability	Chemical Safety
		Consumer Financial Protection
		<b>Privacy &amp; Data Security</b>
	Stakeholder Opposition	Product Safety & Quality
		Responsible Investment
	Social Opportunities	Community Relations
		Controversial Sourcing
		Access to Finance
		Access to Health Care

3 Pillars	10 Themes	33 ESG Key Issues
		Opportunities in Nutrition & Health
		Board
		Pay
		Ownership & Control
		Accounting
		Business Ethics
		Tax Transparency
Governance	Corporate Governance	
	Corporate Behavior	

## Risks associated with this Key Issue

- Loss of revenue or unanticipated remediation and litigation costs in the event of a data breach or misuse.
- Damage to reputation in the event of a breach or controversy over how data is used.
- Loss of significant market or forced change in business model if regulatory action restricts how companies may use data.
- Increased costs to comply with new or evolving regulations.

## Privacy & Data Security Key Issue Score

The Privacy & Data Security Key Issue Score evaluates the company's level of exposure to, and management of, risks on this Key Issue. The Key Issue Score on this Key Issue is based on the Exposure Score and the Management Score using the formula below. The Exposure Score and the Management Score are combined such that a higher level of exposure requires a higher level of demonstrated management capability in order to achieve the same overall Key Issue Score.

$$KI_i = 7 - (\max(EXP_i, 2) - MGMT_i)$$

Where:

- $KI_i$  is the Key Issue Score for company  $i$ .
- $EXP_i$  is the Exposure Score for company  $i$ .
- $MGMT_i$  is the Management Score for company  $i$ .

## Privacy & Data Security Management Score

The Privacy & Data Security Management Score evaluates the company's ability to manage its exposure to risks on this Key Issue. It is based on the Management Score category listed below, modified by Controversies. These scores are derived from data points that are scored on a 0-10 scale, with 10 corresponding to best practice, and 0 corresponding to lack of management. Refer to Section 3.3, Analyzing risk management, of "ESG Ratings Methodology" for additional details. Sources are company disclosures except where otherwise indicated. The following formula is used to calculate the Privacy & Data Security Management Score - Excluding Controversies:

$$MGMT_{PDS,i} = PRA_{PDS,i}$$

Where:

- $MGMT_{PDS,i}$  is the Privacy & Data Security Management Score - Excluding Controversies for company  $i$ .
- $PRA_{PDS,i}$  is the Performance Score for company  $i$ .

The following data points, without constituting an exhaustive list, are representative of the inputs to the Management Score and are used in the Management Score calculation:

### Management Score category: Practices Score

- **Scope of information security management system certifications.**  
**Definition:** The scope of the company's information security management system certification to widely recognized standards. Best practice is for most (over 80%) of owned operations to be certified to widely recognized standards, such as ISO 27001, TRUSTe, Privacy Mark and SSAE16 soc2.
- **Type of information security management system certification.**  
**Definition:** The type of information security management system certification obtained by the company (e.g., ISO 27001, TRUSTe, Privacy Mark, SSAE16 soc2 or another standard).
- **Scope of employee training on privacy and data security.**

**Definition:** The scope of the training employees receive on data security or privacy-related risks and procedures. Best practice is for training to be provided to all employees, including contractors.

- **Responsibility for privacy and data security.**

**Definition:** The group (board-level committee, C-suite or executive committee, or special task force or risk officer) responsible for the company's privacy and data security strategy and performance.

- **Measures to address data breaches.**

**Definition:** The scope of the data breach or incident response plan the company has in place, including whether the plan is proactive, reactive or limited in scope.

- **Frequency of audits of information security system.**

**Definition:** The frequency with which the company audits its information security policies and systems.

- **Collection, usage and retention of customer information.**

**Definition:** Indicates whether the company commits to the principle of minimizing the amount of data handled on its customers and other individuals and does not collect personal data from third parties (except when required by law).

- **Consent policy for use of consumer data for secondary purposes.**

**Definition:** The company's policy on obtaining consent before it rents, sells or provides personal data to third parties for purposes other than completing transactions/services.

- **Rights provided to consumers regarding the control of their data.**

**Definition:** The extent of the rights provided by the company to individuals regarding the access, rectification and deletion of individuals' data.

- **Scope of data protection policy.**

**Definition:** Indicates whether the company's data protection policy governs all or select business lines. A data protection policy must contain at least the following basic provisions: (1) clarifying collection purposes, (2) clarifying the means by which the company collects data, and (3) clarifying whether third parties have access to data and for what purposes.

- **Data protection programs covering suppliers and business partners.**

**Definition:** The extent of the company's data protection or privacy programs covering suppliers and business partners that handle the company's data or have access to the company's network. Best practice is for them to be required to have data protection policies or abide by the company's policy and for inspections to be conducted to verify their compliance.

## Controversies

A controversy deduction ranging from 0 to 5 points is subtracted from the overall Management Score, based on the severity and type of controversies facing the company on this Key Issue. The following categories of controversies are used in the assessment:

- Privacy and data security controversies.

For more details on how controversies are included in the MSCI ESG Ratings model, refer to Section 3.3.2, Controversies cases, of "ESG Ratings Methodology."

## Privacy & Data Security Exposure Score

The Privacy & Data Security Exposure Score evaluates the company's exposure to risks on this Key Issue. It is based on the product of the Business and Company-Specific Exposure Scores, combined with the Geographic Exposure Score. The Geographic Exposure Score functions as a multiplier on the Business Exposure Score and Company Specific Exposure Score, with an impact ranging from -50% to +50%. The Business Exposure Score and Geographic Exposure Score are scored on a 0-10 scale, with 10 corresponding to the highest risk and 0 corresponding to the lowest risk. Refer to Section 3.2, Analyzing risk exposure, of "ESG Ratings

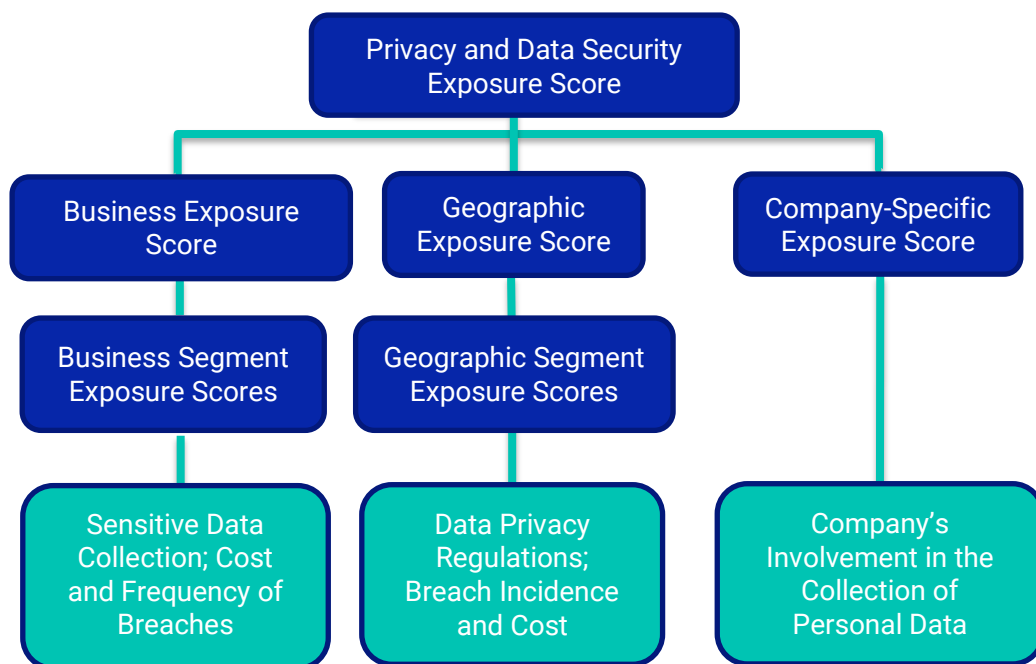
Methodology” for additional details. The following formula is used in the Exposure Score calculation:

$$EXP_{PDS,i} = (BUS_{PDS,i} * COM_{PDS,i})(1 + 0.1(GEO_{PDS,i} - 5))$$

Where:

- $EXP_{PDS,i}$  is the Privacy & Data Security Exposure Score of company  $i$ .
- $BUS_{PDS,i}$  is the Business Exposure Score of company  $i$ .
- $COM_{PDS,i}$  is the Company-Specific Exposure Score of company  $i$ .
- $GEO_{PDS,i}$  is the Geographic Exposure Score of company  $i$ .

## Exhibit 2: Exposure Score components



## Business Exposure Score

The Business Exposure Score is a weighted average of the Business Exposure Scores of a company’s business segments. Scores are weighted by the proportion of a company’s total revenue in each business segment, using the following formula to calculate the Business Exposure Score:



$$BUS_{PDS,i} = \sum_{j=1}^{n_i} w_{Revenue,i,j} BSE_{PDS,j}$$

Where:

- $BSE_{PDS,j}$  is the Business Segment Exposure Score for business segment  $j$ .
- $w_{Revenue,i,j}$  is the weight of business segment  $j$  for company  $i$  based on the contribution to total company revenue.
- $n_i$  is the number of business segments of company  $i$ .

## Business Segment Exposure Scores

The Business Segment Exposure Score of a business segment is based on a mapping of the business segment as disclosed by the company to a corresponding business activity. MSCI ESG Research uses the Standard Industrial Classification (SIC) system along with industry-specific adjustments to define business activities. The score associated with a business activity is used to calculate a Business Segment Exposure Score. Each business activity score is determined by the business activity's sensitivity to data breaches and certain characteristics of its data breaches, using the following formula:

$$BSE_{PDS,j} = \frac{SEN_j + DB_j}{2}$$

Where:

- $BSE_{PDS,j}$  is the Business Segment Exposure Score for business segment  $j$ .
- $SEN_j$  is the Sensitivity Score for business activity  $j$ .
- $DB_j$  is the Data Breach Score for business activity  $j$ .

The Sensitivity Score of a business activity is determined by a qualitative assessment of the following factors.

- Handling of sensitive data such as Social Security numbers, dates of birth, financial account information, health data or locations.
- Involvement in business activities such as selling advertising or selling access to user data.

The Data Breach Score of a business activity is calculated as the average of the Breach Frequency Score and the Breach Cost Score, as shown below:

$$DB_j = \frac{BF_j + BC_j}{2}$$

Where:

- $DB_j$  is the Data Breach Score for business activity  $j$ .
- $BF_j$  is the Breach Frequency Score for business activity  $j$ .
- $BC_j$  is the Breach Cost Score for business activity  $j$ .

The Breach Frequency Score indicates the ratio of total breach incidents as a proportion of average sales in the business activity. The Breach Cost Score indicates the cost of data breaches per lost or stolen record in a business activity. Both these indicators are scored on a 0-10 scale, with 10 corresponding to the highest risk and 0 corresponding to the lowest risk.

## Geographic Exposure Score

The Geographic Exposure Score is a weighted average of the Geographic Segment Exposure Scores of the countries and regions in which a company operates. Scores are weighted by the proportion of a company's total revenue in each geographic segment through the following equation:

$$GEO_{PDS,i} = \sum_{r=1}^{n_i} w_{Revenue,i,r} GSE_{PDS,r}$$

Where:

- $GSE_{PDS,r}$  is the Geographic Segment Exposure Score in region  $r$ .
- $w_{Revenue,i,r}$  is the weight of total revenue in region  $r$  for company  $i$ .
- $n_i$  is the number of geographic segments for company  $i$ .

For geographic segments disclosed as regions (example: Asia Pacific), a nominal GDP-weighted country aggregation is used to calculate region-level scores, using the following equation:

$$GSE_{PDS,r} = \sum_{c=1}^{n_r} w_{GDP,r,c} GSE_{PDS,c}$$

Where:

- $GSE_{PDS,c}$  is the Geographic Segment Exposure Score of country  $c$ .
- $w_{GDP,r,c}$  is the specific weight of country  $c$  within region  $r$ .

## Geographic Segment Exposure Scores

The Geographic Segment Exposure Score is determined by assessing a country's privacy and data security regulation and certain characteristics of its data breaches, using the following formula:

$$GSE_{PDS,c} = \frac{REG_c + DB_c}{2}$$

Where:

- $REG_c$  is the Regulatory Score for country  $c$ .
- $DB_c$  is the Data Breach Score for country  $c$ .

The Regulatory Score of a country is determined by a qualitative assessment of the following factors:

- Level of restriction in national privacy and data security regulation relative to global standards.
- Likelihood of regulatory change in the next few years.

The Data Breach Score of a country is the average of the Breach Incidence Score and the Breach Cost per Company Score, as shown below.

$$DB_c = \frac{BI_c + BCC_c}{2}$$

Where:

- $DB_c$  is the Data Breach Score for country  $c$ .
- $BI_c$  is the Breach Incidence Score for country  $c$ .
- $BCC_c$  is the Breach Cost per Company score for country  $c$ .

The Breach Incidence Score indicates the total number of breaches recorded in the country or region. The Breach Cost per Company Score indicates the average cost incurred per company operating in the country or region.

The Data Breach Score, Breach Incidence Score and Breach Cost per Company Score are measured on a 0-10 scale, with 10 corresponding to the highest risk and 0 corresponding to the lowest risk.

## Company-Specific Exposure Score

The Company Specific Exposure Score is calculated based on whether the company is involved in the collection of personal data, as shown below:

If a company is involved in the collection of personal data, the score is calculated using the following formula:

$$COM_{PDS,k} = 1$$

Where:

- $COM_{PDS,k}$  is the Company-Specific Exposure Score of company  $k$ .

If a company is not involved in the collection of personal data, the score is calculated using the following formula:

$$COM_{PDS,k} = 0.5$$

## Data Sources

The following sources are used to determine the Privacy & Data Security Exposure Score:

Ponemon Institute and IBM's Cost of a Data Breach report series, Verizon's Data Breach Investigations Report, Refinitiv, MSCI ESG Research, company disclosures.

## Contact us

[msci.com/contact-us](https://www.msci.com/contact-us)

### AMERICAS

United States	+ 1 888 588 4567 *
Canada	+ 1 416 687 6270
Brazil	+ 55 11 4040 7830
Mexico	+ 52 81 1253 4020

### EUROPE, MIDDLE EAST & AFRICA

South Africa	+ 27 21 673 0103
Germany	+ 49 69 133 859 00
Switzerland	+ 41 22 817 9777
United Kingdom	+ 44 20 7618 2222
Italy	+ 39 02 5849 0415
France	+ 33 17 6769 810

### ASIA PACIFIC

China	+ 86 21 61326611
Hong Kong	+ 852 2844 9333
India	+ 91 22 6784 9160
Malaysia	1800818185 *
South Korea	+ 82 70 4769 4231
Singapore	+ 65 67011177
Australia	+ 612 9033 9333
Taiwan	008 0112 7513 *
Thailand	0018 0015 6207 7181 *
Japan	+ 81 3 4579 0333

\* toll-free

### About MSCI

MSCI is a leading provider of critical decision support tools and services for the global investment community. With over 50 years of expertise in research, data and technology, we power better investment decisions by enabling clients to understand and analyze key drivers of risk and return and confidently build more effective portfolios. We create industry-leading research-enhanced solutions that clients use to gain insight into and improve transparency across the investment process.

### About MSCI ESG Research Products and Services

MSCI ESG Research products and services are provided by MSCI ESG Research LLC, and are designed to provide in-depth research, ratings and analysis of environmental, social and governance-related business practices to companies worldwide. ESG ratings, data and analysis from MSCI ESG Research LLC. are also used in the construction of the MSCI ESG Indexes. MSCI ESG Research LLC is a Registered Investment Adviser under the Investment Advisers Act of 1940 and a subsidiary of MSCI Inc.

To learn more, please visit [www.msci.com](https://www.msci.com).

## Notice and disclaimer

This document and all of the information contained in it, including without limitation all text, data, graphs, charts (collectively, the "Information") is the property of MSCI Inc. or its subsidiaries (collectively, "MSCI"), or MSCI's licensors, direct or indirect suppliers or any third party involved in making or compiling any Information (collectively, with MSCI, the "Information Providers") and is provided for informational purposes only. The Information may not be modified, reverse-engineered, reproduced or disseminated in whole or in part without prior written permission from MSCI. All rights in the Information are reserved by MSCI and/or its Information Providers.

The Information may not be used to create derivative works or to verify or correct other data or information. For example (but without limitation), the Information may not be used to create indexes, databases, risk models, analytics, software, or in connection with the issuing, offering, sponsoring, managing or marketing of any securities, portfolios, financial products or other investment vehicles utilizing or based on, linked to, tracking or otherwise derived from the Information or any other MSCI data, information, products or services.

The user of the Information assumes the entire risk of any use it may make or permit to be made of the Information. NONE OF THE INFORMATION PROVIDERS MAKES ANY EXPRESS OR IMPLIED WARRANTIES OR REPRESENTATIONS WITH RESPECT TO THE INFORMATION (OR THE RESULTS TO BE OBTAINED BY THE USE THEREOF), AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EACH INFORMATION PROVIDER EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES (INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF ORIGINALITY, ACCURACY, TIMELINESS, NON-INFRINGEMENT, COMPLETENESS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE) WITH RESPECT TO ANY OF THE INFORMATION.

Without limiting any of the foregoing and to the maximum extent permitted by applicable law, in no event shall any Information Provider have any liability regarding any of the Information for any direct, indirect, special, punitive, consequential (including lost profits) or any other damages even if notified of the possibility of such damages. The foregoing shall not exclude or limit any liability that may not by applicable law be excluded or limited, including without limitation (as applicable), any liability for death or personal injury to the extent that such injury results from the negligence or willful default of itself, its servants, agents or sub-contractors.

Information containing any historical information, data or analysis should not be taken as an indication or guarantee of any future performance, analysis, forecast or prediction. Past performance does not guarantee future results.

The Information may include "Signals," defined as quantitative attributes or the product of methods or formulas that describe or are derived from calculations using historical data. Neither these Signals nor any description of historical data are intended to provide investment advice or a recommendation to make (or refrain from making) any investment decision or asset allocation and should not be relied upon as such. Signals are inherently backward-looking because of their use of historical data, and they are not intended to predict the future. The relevance, correlations and accuracy of Signals frequently will change materially.

The Information should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. All information is impersonal and not tailored to the needs of any person, entity or group of persons.

None of the Information constitutes an offer to sell (or a solicitation of an offer to buy), any security, financial product or other investment vehicle or any trading strategy.

It is not possible to invest directly in an index. Exposure to an asset class or trading strategy or other category represented by an index is only available through third party investable instruments (if any) based on that index. MSCI does not issue, sponsor, endorse, market, offer, review or otherwise express any opinion regarding any fund, ETF, derivative or other security, investment, financial product or trading strategy that is based on, linked to or seeks to provide an investment return related to the performance of any MSCI index (collectively, "Index Linked Investments"). MSCI makes no assurance that any Index Linked Investments will accurately track index performance or provide positive investment returns. MSCI Inc. is not an investment adviser or fiduciary and MSCI makes no representation regarding the advisability of investing in any Index Linked Investments.

Index returns do not represent the results of actual trading of investable assets/securities. MSCI maintains and calculates indexes, but does not manage actual assets. The calculation of indexes and index returns may deviate from the stated methodology. Index returns do not reflect payment of any sales charges or fees an investor may pay to purchase the securities underlying the index or Index Linked Investments. The imposition of these fees and charges would cause the performance of an Index Linked Investment to be different than the MSCI index performance.

The Information may contain back tested data. Back-tested performance is not actual performance, but is hypothetical. There are frequently material differences between back tested performance results and actual results subsequently achieved by any investment strategy.

Constituents of MSCI equity indexes are listed companies, which are included in or excluded from the indexes according to the application of the relevant index methodologies. Accordingly, constituents in MSCI equity indexes may include MSCI Inc., clients of MSCI or suppliers to MSCI. Inclusion of a security within an MSCI index is not a recommendation by MSCI to buy, sell, or hold such security, nor is it considered to be investment advice.

Data and information produced by various affiliates of MSCI Inc., including MSCI ESG Research LLC and Barra LLC, may be used in calculating certain MSCI indexes. More information can be found in the relevant index methodologies on [www.msci.com](http://www.msci.com).

MSCI receives compensation in connection with licensing its indexes to third parties. MSCI Inc.'s revenue includes fees based on assets in Index Linked Investments. Information can be found in MSCI Inc.'s company filings on the Investor Relations section of [msci.com](http://www.msci.com).

MSCI ESG Research LLC is a Registered Investment Adviser under the Investment Advisers Act of 1940 and a subsidiary of MSCI Inc. Neither MSCI nor any of its products or services recommends, endorses, approves or otherwise expresses any opinion regarding any issuer, securities, financial products or instruments or trading strategies and MSCI's products or services are not a recommendation to make (or refrain from making) any kind of investment decision and may not be relied on as such, provided that applicable products or services from MSCI ESG Research may constitute investment advice. MSCI ESG Research materials, including materials utilized in any MSCI ESG Indexes or other products, have not been submitted to, nor received approval from, the United States Securities and Exchange Commission or any other regulatory body. MSCI ESG and climate ratings, research and data are produced by MSCI ESG Research LLC, a subsidiary of MSCI Inc. MSCI ESG Indexes, Analytics and Real Estate are products of MSCI Inc. that utilize information from MSCI ESG Research LLC. MSCI Indexes are administered by MSCI Limited (UK).

Please note that the issuers mentioned in MSCI ESG Research materials sometimes have commercial relationships with MSCI ESG Research and/or MSCI Inc. (collectively, "MSCI") and that these relationships create potential conflicts of interest. In some cases, the issuers or their affiliates purchase research or other products or services from one or more MSCI affiliates. In other cases, MSCI ESG Research rates financial products such as mutual funds or ETFs that are managed by MSCI's clients or their affiliates, or are based on MSCI Inc. Indexes. In addition, constituents in MSCI Inc. equity indexes include companies that subscribe to MSCI products or services. In some cases, MSCI clients pay fees based in whole or part on the assets they manage. MSCI ESG Research has taken a number of steps to mitigate potential conflicts of interest and safeguard the integrity and independence of its research and ratings. More information about these conflict mitigation measures is available in our Form ADV, available at <https://adviserinfo.sec.gov/firm/summary/169222>.

Any use of or access to products, services or information of MSCI requires a license from MSCI. MSCI, Barra, RiskMetrics, IPD and other MSCI brands and product names are the trademarks, service marks, or registered trademarks of MSCI or its subsidiaries in the United States and other jurisdictions. The Global Industry Classification Standard (GICS) was developed by and is the exclusive property of MSCI and S&P Global Market Intelligence. "Global Industry Classification Standard (GICS)" is a service mark of MSCI and S&P Global Market Intelligence.

MIFID2/MIFIR notice: MSCI ESG Research LLC does not distribute or act as an intermediary for financial instruments or structured deposits, nor does it deal on its own account, provide execution services for others or manage client accounts. No MSCI ESG Research product or service supports, promotes or is intended to support or promote any such activity. MSCI ESG Research is an independent provider of ESG data.

Privacy notice: For information about how MSCI collects and uses personal data, please refer to our Privacy Notice at <https://www.msci.com/privacy-pledge>.

Any use of or access to products, services or information of MSCI requires a license from MSCI. MSCI, Barra, RiskMetrics, IPD and other MSCI brands and product names are the trademarks, service marks, or registered trademarks of MSCI or its subsidiaries in the United States and other jurisdictions. The Global Industry Classification Standard (GICS) was developed by and is the exclusive property of MSCI and S&P Global Market Intelligence. "Global Industry Classification Standard (GICS)" is a service mark of MSCI and S&P Global Market Intelligence.

MIFID2/MIFIR notice: MSCI ESG Research LLC does not distribute or act as an intermediary for financial instruments or structured deposits, nor does it deal on its own account, provide execution services for others or manage client accounts. No MSCI ESG Research product or service supports, promotes or is intended to support or promote any such activity. MSCI ESG Research is an independent provider of ESG data.

Privacy notice: For information about how MSCI collects and uses personal data, please refer to our Privacy Notice at <https://www.msci.com/privacy-pledge>.