Global Privacy Policy

1. Introduction

Venator Materials PLC, its subsidiaries and affiliates located globally (collectively, “Venator” or the "Company"), Process and Transfer Personal Data, to the extent necessary or appropriate for the administration of your employment relationship or any other specified, explicit and legitimate purposes. In this regard, and in compliance with this Global Privacy Policy (“Policy”), the Company strives to comply with Applicable Laws to the extent they apply to associates and to other individuals.

2. Scope

This Global Privacy Policy (“Policy”) provides associates with information about how the Company Processes and Transfers Personal Data locally, regionally and globally, including but not limited to Transfers to the U.S. in accordance with Applicable Laws. The HR Team, the Privacy Team, or, where applicable, the local Data Protection Officer (“DPO”), can provide further information about Company policies and procedures that relate to Personal Data.

3. Definitions

Applicable Laws

The principles of data protection laws as set forth in the European General Data Protection Regulation (“GDPR”), Privacy Shield principles or local data protection legislation, whichever is stricter.

Personal Data

Any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity. Categories of Personal Data collected and Processed by the Company or a third party are identified in Section 5 below.

Data Controller

The entity that alone or jointly with others determines the purposes and means of the Processing of Personal Data.

Data Processor

The entity that Processes Personal Data on behalf of the Data Controller.

Process/Processed/Processing

Any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Transfer/Transferred/Transferring

When one party or the Company makes Personal Data available, by whatever means, to another party or the Company.

4. Privacy Shield Statement

With respect to the Personal Data of associates, the Company recognizes that there is an "omnibus" data protection regime pursuant to Applicable Laws. The Applicable Laws generally restrict the Transfer of Personal Data of associates in the EU or Switzerland to the U.S., unless there is "adequate protection" for such Personal Data when it is received in the U.S. In order to address this restriction, the Company adhere to the U.S./EU and U.S./Swiss Privacy Shield principles published by the U.S. Federal Trade Commission with respect to the Personal Data the Company receives in the U.S. Further information about the Privacy Shield can be found in the Company's Privacy Shield Policy, located on the GDPR intranet page on VenNet, or on the U.S. Federal Trade Commission website at https://www.privacyshield.gov/welcome.

5. Personal Data Defined and Collected

The types of Personal Data that the Company may receive, Process and Transfer locally, regionally and globally, including Transfers to the U.S., or disclose to other Venator companies or third-party organizations providing administration or other services to the Company, have been divided into Personal Data Categories. The Personal Data Categories trigger increased restriction requirements, based on Personal Data sensitivity, for internal access privileges and physical data handling protections required for associates whose valid business related tasks include the handling of Personal Data. These Personal Data Categories were designed to (i) assist associates with quickly recognizing the relative sensitivity of such Personal Data with regard to the personal rights of an individual for internal and external handling and protection purposes and (ii) enhance awareness training of the permissible and limited purposes of access, use and disclosure for each Personal Data Category, in order to protect it from theft, compromise, inappropriate use and viewing by unauthorized associates or other individuals.

The Personal Data Categories are as follows:

Category 1 (Green) - Individual's Contact and Business Identification Data

Individual's name and business related contact information such as work telephone number(s), business address and email address;

Category 2 (Yellow) - Company Created Personal Data

Information related to job and salary such as compensation data; bonuses and incentives; general information regarding benefits; retirement pensions; performance; compliance with EHS policies, procedures, standards and guidelines and related investigations; training and development and compliance with Company policies, procedures, standards and guidelines and related investigations;

Category 3 (Orange) - Personal Data Provided by the Individual

Information related to location data or online identifier such as home address; home and any personal telephone numbers; email and IP addresses; work and educational background; business travel and expenses; and image;

Category 4 (Red) - Personal Data That May Be Considered Sensitive

Depending upon the Applicable Laws, Personal Data that may be considered sensitive data, which includes government issued identification information; race or ethnic origin, religious beliefs; genetic information; physical or mental health condition or disability; sexual orientation; personal banking or payment card information; trade union membership; criminal history and any punishment received for a proven offense or any other Personal Data that severely impedes personal rights of the affected individual.

In addition, if an associate needs to obtain a visa to work in the U.S. or elsewhere, the Company may ask the associate, and any accompanying family members, to provide additional Personal Data or family information to the Company to assist with the visa applications. The Company also may receive certain information regarding an associate's spouse, family members or other dependents for emergency contact (if voluntarily provided) and for benefits administration purposes.

The Company receives Personal Data that is "sensitive" within the meaning and to the extent permitted under Applicable Laws, such as when it is necessary for the performance of the employment or contractual relationship. In particular, the Company may receive and Process Personal Data that is sensitive related to an associate's health and/or disabilities for the business purposes of administration of health benefits, medical surveillance programs, leave administration, or work duties accommodation.

Personal Data may be collected prior to the commencement of employment such as during the recruitment process and also throughout an associate's employment by online means and/or in paper form.

6. The Company's Uses of Personal Data

The Company may Process and Transfer Personal Data locally, regionally and globally, including in the U.S., in connection with an associate for purposes, as permitted by Applicable Laws, such as the following:

- Emergency Contacts
- Consideration for employment or promotion
- Administration of personnel and work duties
- Performance management and training and development
- Leave administration
- Facilitating travel and processing expense reports
- Administration of compensation, bonus, pension, benefits, and incentive programs
- Administration of health benefits, workers' compensation, and medical surveillance programs
- Administration of executive compensation-related programs
- Workflow management and continuity
- Budgeting and planning
- Succession planning
- Sale, merger or reorganization of the business
- Business-related personal surveys
- Processing visa applications and work permits
- Compliance and legal considerations requiring investigating, auditing, and enforcing the Company's policies, procedures, guidelines, and standards
- Compliance with applicable social, tax, and other legal requirements and regulations
- IT Security measures to prevent external and/or internal intrusion
- Company network access and IT support
- Business related communication

- Facilitating social collaboration on the Company's network
- Preserving or defending the Company's legal rights following demands or during business related litigation
- Administration of grievances and / or claims
- Personal contact directories
- Mailing of Company communications

For prevention, detection or investigation of external and/or internal intrusions to the Company's IT systems the Company may Process and Transfer Personal Data such as log files or IP addresses to the extent that is permitted by Applicable Laws.

Further, the Company may Process Personal Data as part of any Ethics & Compliance investigation. This includes Personal Data about the person making the complaint (to the extent that person has identified themselves), Personal Data about any individual who is the subject of the complaint and Personal Data of any other individual who assists us with the Company's investigations. The nature of Personal Data Processed depends on the nature of the report received and it may include sensitive Personal Data. The Company will only retain such Personal Data for as long as it is relevant for the Ethics & Compliance investigation or necessary for legal reasons.

7. Personal Data Transfers and Processing

In order to Process Personal Data, it may be necessary for the Company to store it in the Company's Human Resources information system or other Company computerized or electronic systems or platforms and Transfer it locally, regionally and globally, including to the U.S., or disclose it to other Venator companies or third-party organizations providing administration or other services to the Company, subject to appropriate safeguards.

As necessary in connection with these purposes, the Human Resources Team, functional managers or supervisors may Process and Transfer Personal Data in connection with their job responsibilities and valid business related tasks. If and where permitted by Applicable Laws, Personal Data also may be accessed by certain associates within the Company related to business related IT traffic and content analysis, and operating systems monitoring and maintenance. The Company takes appropriate steps designed to ensure that such personnel maintain confidentiality with respect to Personal Data.

The Company intend to protect Personal Data in line with the Applicable Laws regardless of whether the recipients are located in or out of the EU or Switzerland, including in countries that may not offer the same level of protection of Personal Data or countries that do not have national laws providing the same level of Personal Data protection. Any Transfer of Personal Data to a country that does not provide for an adequate level of data protection within the meaning of the Applicable Laws, will be made on the basis of (i) associate consent, (ii) a Data Transfer Agreement, (iii) the Privacy Shield Program, or (iv) other appropriate safeguards in accordance with Applicable Laws or Company policy.

8. Notice and Choice

The Company intends to use Personal Data for the purposes for which such Personal Data was originally collected and do not intend to disclose Personal Data to any third party for an inconsistent purpose, except with the appropriate consent of the affected individuals as permitted under the Privacy Shield principles or local standards in accordance with Applicable Laws, or for the Processing of the Personal Data by an external Processor who provides sufficient guarantees to the Company related to the technical and organizational measures taken related to the protection of the Personal Data.

Any list required by Applicable Laws of the names and addresses of third-party Processors and internal computerized or electronic systems utilized by the Company as well as any required list of the countries Personal Data is Transferred to can be obtained from the Privacy Team.

9. Data Security and Data Integrity

The Company has implemented appropriate technical and organizational security measures to protect Personal Data from loss, misuse, unauthorized access, disclosure, or unauthorized alteration or destruction. Associates also are subject to certain confidentiality obligations related to the handling and protection of Personal Data and may be disciplined or terminated if they fail to meet these obligations.

The Company also maintains procedures designed to help ensure, to the extent appropriate or required by the Applicable Laws, that Personal Data is reliable for its intended use and accurate, complete, and current and that the individual can exercise their right to access or erasure of Personal Data. In this regard, the individual is encouraged to update their own Personal Data when appropriate to keep it accurate, complete, and current. The Company retains Personal Data only for so long as is required by the Company's Document Retention Procedure or as permitted by Applicable Laws.

10. Access to Personal Data

Associates or other individuals have the right to access and review their own Personal Data in accordance with the Global Privacy Procedure and the Applicable Laws to verify its accuracy and lawful uses, which can include inquiring into the purposes of Processing, the categories of Personal Data concerned, and the third-parties or categories of third-parties to whom their Personal Data is disclosed. Where appropriate or required by Applicable Laws, with respect to Personal Data maintained by or on behalf of the Company, an associate may update or correct any inaccurate Personal Data about themselves. Subject to the Applicable Laws, an associate may also request that their Personal Data be blocked or deleted. In some circumstances, however, access may be denied where the burden or expense of providing access would be disproportionate to the risks to the associate's privacy, where the rights of others would be violated, where confidential commercial information or succession planning or re-organization information would be revealed, or where a compliance, legal, or regulatory matter, function or privilege would be prejudiced or jeopardized. After leaving the Company, the Company may be entitled or required by law to continue to Process an associate's Personal Data in connection with the employment relationship or the Company's legal responsibilities.

An associate should send requests for access, amendment or deletion to their Personal Data, in writing or via email, to the Privacy Team, identified below or Data Protection Officer.

11. Disclosures Required or Permitted By Applicable Laws

Regardless of any other provisions in this Policy, the Company may disclose or otherwise Process Personal Data in the context of any sale, merger, transaction or reorganization involving all or a portion of the business, or for the purpose of audits conducted by outside auditors as is necessary to satisfy statutory requirements, or in other circumstances without which non-disclosure would prejudice the legitimate interests of the Company, or as may be required or permitted by Applicable Laws. It is the Company's intent to implement appropriate measures, such as pseudonymisation and data minimization, to seek appropriate protection of Personal Data in these types of transactions.

The Company may also regularly disclose Personal Data to government agencies and regulators (e.g., tax authorities), social organizations (e.g., the social security administration), human resources benefits providers (e.g., health insurers), travel-related third-parties (e.g., to book a flight, hotel room or rental car), courts and other tribunals and government authorities or to the extent required by lawful requests from public authorities to meet national security or enforcement requirements or other applicable legal obligations, in accordance with the Applicable Laws.

If and where requested by the Applicable Laws the Company will not disclose an associate's Personal Data to any third party without having obtained their written consent.

12. Personal Data about Dependents and Related Persons

If an associate provides the Company with Personal Data about their dependents, family members and/or related persons (e.g., for benefits administration and/or emergency contact purposes), it is the associate's responsibility to inform such individuals about the Processing of their Personal Data by the Company for those purposes and in the manner described in this Policy, about their rights of access, correction and deletion in accordance with the Applicable Laws , as well as to obtain their consent, where necessary, to the Processing (including the Transfer to countries that may not provide the same level of protection of Personal Data as in their home country) of their Personal Data as is set out in this Policy.

13. Associate Inquiries and Reporting Concerns

An associate can inquire into any issue regarding Applicable Laws with the Privacy Team or the local Data Protection Officer, where existent. Concerns or access requests can also be sent to:

E-mail: privacy@venatorcorp.com

For associates in the EU, additional information about the complaint process for EU associates is provided in the Company's Privacy Shield Policy, which is located on the Company's intranet site.

Document Revision History

Policy:	Privacy
Document Reference:	PRIV-001
Issue Date:	2018-06-06
Index Number:	11.1
Values:	Integrity, Zero Harm, Teamwork, Innovation, Performance

Allgemeine Datenschutzrichtlinien

1. Einleitung

Die Venator Materials PLC sowie ihre weltweit ansässigen Tochtergesellschaften und verbundenen Unternehmen (zusammen die „Venator“ oder das „Unternehmen“) verarbeiten und übermitteln personenbezogene Daten in dem Umfang, wie es die Erfüllung Ihres Beschäftigungsverhältnisses erforderlich und angemessen ist, sowie für andere festgelegte, eindeutige und rechtmäßige Zwecke. In diesem Zusammenhang ist das Unternehmen bestrebt, die Anwendbaren Gesetze, sowie diese allgemeine Datenschutzrichtlinie, soweit diese für Mitarbeiter und andere Personen Anwendung finden, einzuhalten.

2. Geltungsbereich

Diese allgemeine Datenschutzrichtlinie (die „Richtlinie“) informierten die Mitarbeiter darüber, wie das Unternehmen personenbezogene Daten lokal, regional und global verarbeitet und übermittelt. Das beinhaltet ggf. auch Datentransfers in die USA unter Beachtung der Anwendbaren Gesetze. Das HR- und das Privacy Team oder ggf. der lokale Datenschutzbeauftragte stellen Ihnen gerne weitere Informationen über die Richtlinien und Verfahren des Unternehmens in Bezug auf personenbezogene Daten bereit.

3. Definitionen

Anwendbare Gesetze

Die in der Europäischen Datenschutzgrundverordnung („DSGVO“) niedergelegten Prinzipien der Datenschutzgesetze, die Privacy-Shield-Grundsätze oder die lokalen Datenschutzgesetz; je nachdem, welches Gesetz strenger ist.

Personenbezogene Daten

Jedwede Informationen in Bezug auf eine identifizierte oder identifizierbare natürliche Person. Eine identifizierbare Person ist eine Person, die direkt oder indirekt insbesondere anhand einer Kennung wie ein Name, eine Identifikationsnummer, Standortdaten, eine Online-Kennung oder einer oder mehrere Faktoren, die für ihre physische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität spezifisch sind, identifiziert werden kann. Die Kategorien an personenbezogenen Daten, die das Unternehmen oder eine dritte Partei erfassen und verarbeiten, sind in unten stehendem Abschnitt 5 angegeben.

Verantwortlicher

Das Unternehmen, das alleine oder zusammen mit anderen die Zwecke und die Mittel der Verarbeitung personenbezogener Daten festgelegt.

Datenverarbeiter

Das Unternehmen, das im Auftrag des Verantwortlichen personenbezogene Daten verarbeitet.

Verarbeiten / verarbeitet

Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder Vorgangsreihe, im Zusammenhang mit personenbezogenen Daten. Hierzu zählen personenbezogene Daten zu erfassen, zu protokollieren, zu organisieren, zu strukturieren, aufzubewahren, zu anzupassen oder zu ändern, wiederherzustellen, einzusehen, zu verwenden, mittels Übertragung offenzulegen, zu verbreiten oder in anderer Form zur Verfügung zu stellen, abzugleichen oder zu kombinieren, einzuschränken, zu löschen oder zu vernichten.

Übertragung / Übertragen

Wenn eine Partei oder das Unternehmen mittels welcher Mittel auch immer einer anderen Partei oder dem Unternehmen personenbezogene Daten bereitstellt.

4. Privacy-Shield-Erklärung

Dem Unternehmen ist in Bezug auf personenbezogene Daten der Mitarbeiter bewusst, dass es eine Vielzahl von Datenschutzsystemen gibt, die den Anwendbaren Gesetzen unterliegen. Die Anwendbaren Gesetze schränken den Transfer der Personenbezogenen Daten von Mitarbeitern aus der EU oder der Schweiz weitestgehend ein, soweit es nicht ein „adäquates Schutzniveau“ für diese personenbezogenen Daten besteht, wenn diese in die USA übermittelt werden. Um dieser Beschränkung gerecht zu werden, hält das Unternehmen die zwischen den USA / EU und USA / Schweiz vereinbarten Privacy-Shield-Grundsätze ein. Diese wurden von der amerikanischen Federal Trade Commission in Bezug auf personenbezogene Daten, die das Unternehmen in die USA übermittelt, veröffentlicht. Weitere Informationen über das „Privacy Shield“ können in den Datenschutzrichtlinien des Unternehmens auf der DSGVO Intranetseite auf dem oder auf der Website der amerikanischen Federal Trade Commission unter https://www.privacyshield.gov/welcome nachgelesen werden.

5. Festgelegte und erfasste personenbezogene Daten

Die Arten an personenbezogenen Daten, die das Unternehmen möglicherweise lokal, regional und weltweit erhält, verarbeitet und übermittelt – inklusive dem Transfer in die USA – oder der Weitergabe an andere Venator-Unternehmen oder gegenüber dritten Parteien gegenüber, die dem Unternehmen Verwaltungs- oder andere Dienstleistungen bereitstellen, wurden in Kategorien von Personenbezogenen Daten aufgeteilt. Basierend auf der Sensibilität der Personenbezogenen Daten lösen die jeweiligen Kategorien erhöhte Beschränkungen in Bezug auf interne Zugangsrechte und physische Sicherheitsvorkehrungen für Mitarbeiter aus, zu deren berufsbezogenen Aufgaben die Handhabung personenbezogener Daten gehört. Diese Kategorien an Personenbezogenen Daten dienen dazu, (i) die Mitarbeiter dabei zu unterstützen, die jeweilige Sensibilität der Personenbezogenen Daten im Hinblick auf die Persönlichkeitsrechte eines Betroffenen bei der internen und externen Verarbeitung und die erforderlichen Schutzzwecke schnell erkennen zu können und (ii) die Wahrnehmung bezüglich der zulässigen und eingeschränkten Zwecksetzungen in Bezug auf Zugang, Verwendung und Offenlegung für jede Kategorie an personenbezogenen Daten zu verbessern, um diese vor Diebstahl, Beeinträchtigung, unsachgemäße Nutzung und davor zu schützen, von nicht autorisierten Mitarbeitern oder anderen Personen eingesehen werden zu können.

Bei den Kategorien an Personenbezogenen Daten handelt es sich um Folgende:

Kategorie 1 (Grün) – die Kontakt- und Geschäftsidentifikationsdaten einer Person

Der Name und die unternehmensbezogene Kontaktdaten einer Person wie die dienstliche Telefonnummer (n) sowie die Geschäfts- und E-Mail-Adresse.

Kategorie 2 (Gelb) – vom Unternehmen erstellte personenbezogene Daten

Informationen in Bezug auf die Arbeit und das Gehalt wie Daten über Entgelte, Boni und Incentives, allgemeine Informationen in Bezug auf Zusatzleistungen, Rente, Leistung, Einhaltung der EHS-Richtlinien, von Verfahren, Standards und Richtlinien und darauf bezogene Ermittlungen, Schulung und Entwicklung sowie die Einhaltung der Richtlinien, Abläufe, Standards und Orientierungshilfen des Unternehmens und darauf bezogene Ermittlungen.

Kategorie 3 (Orange) – von der Person bereitgestellte personenbezogene Daten

Informationen in Bezug auf Standortdaten oder Online-Kennungen wie die Wohnadresse, dienstliche und private Telefonnummern, E-Mail- und IP-Adressen, Berufs- und Ausbildungshintergrund, Geschäftsreisen und Auslagen und Fotos.

Kategorie 4 (Rot) – als sensibel zu betrachtende personenbezogene Daten

Personenbezogene Daten, die abhängig von den Anwendbaren Gesetzen als sensible Daten betrachtet werden. Das beinhaltet von einer Behörde ausgestellte Identifikationsmerkmale, die ethnische Herkunft, religiöse Überzeugungen, genetische Informationen, Informationen über Physis und Psyche oder Arbeitsunfähigkeit, sexuelle Orientierung, personenbezogene Bank- oder Bezahlkarteninformationen, Mitgliedschaft in einer Gewerkschaft, Vorstrafen und jedwede Strafen für bewiesene Vergehen oder jedwede sonstigen personenbezogenen Daten, die die Persönlichkeitsrechte des Betroffenen schwerwiegend beeinträchtigen können.

Das Unternehmen wird möglicherweise, wenn ein Mitarbeiter ein Arbeitsvisum für die USA oder anderenorts erwirken muss, darüber hinaus den Mitarbeiter oder jedwede begleitenden Familienmitglieder bitten, dem Unternehmen ergänzende Personenbezogene Daten oder Familieninformationen bereitzustellen, um die Visa-Anträge zu unterstützen. Darüber hinaus darf das Unternehmen Informationen in Bezug auf den Ehepartner des Mitarbeiters, dessen Familienmitglieder oder andere Angehörige als Notfallkontakt (wenn freiwillig bereitgestellt) und zur Unterstützung der Verwaltungstätigkeiten entgegennehmen.

Das Unternehmen erhält sensible Daten im Sinne der Anwendbaren Gesetze gemäß dem gesetzlichen Rahmen wenn dies für die Leistung der Beschäftigung oder des Vertragsverhältnisses erforderlich ist. So ist es insbesondere möglich, dass das Unternehmen sensible personenbezogene Daten in Bezug auf die Gesundheit und / oder Arbeitsunfähigkeit eines Mitarbeiters, bezüglich der Verwaltung gesundheitlicher Unterstützung, medizinischer Überwachungsprogramme oder im Rahmen der Abwicklung des Arbeitsverhältnisses erhält.

Es ist möglich, dass Personenbezogene Daten vor dem Beginn des Beschäftigungsverhältnisses wie beispielsweise im Rahmen des Bewerbungsprozesses sowie auch während des Beschäftigungsverhältnisses eines Mitarbeiters online und / oder in Papierform erfasst werden.

6. Verarbeitung von personenbezogenen Daten durch das Unternehmen

Das Unternehmen kann personenbezogene Daten lokal, regional und weltweit einschließlich in den USA in Verbindung mit einem Mitarbeiter zu Zwecken, die gemäß den Anwendbaren Gesetzen zulässigen sind, wie beispielsweise zu Folgendem verarbeiten und übertragen:

- Notfallkontakte
- Berücksichtigung zur Beschäftigung oder Förderung
- Zur Verwaltung des Personals und von Arbeitspflichten
- Leistungsmanagement sowie Schulung und Entwicklung
- Urlaubsverwaltung
- Durchführung von Reisen und Reisekostenabrechnungen
- Verwaltung der Gehalts-, Boni-, Renten-, Zusatzleistungs- und Incentiveprogramme
- Verwaltung von gesundheitlicher Unterstützung, der Arbeitsunfallversicherung und der medizinischen Überwachungsprogramme
- Verwaltung der gehaltsbezogenen Programme für Führungskräfte
- Arbeitsablaufmanagement und Kontinuität
- Budget und Planung
- Nachfolgeplanung
- Veräußerung, Fusion und Reorganisation des Geschäfts
- Geschäftsbezogene persönliche Umfragen
- Visaanträge und Arbeitsgenehmigungen verarbeiten
- Einhaltung und rechtliche Betrachtungen, für die Ermittlungen und Überprüfungen erforderlich sind, sowie Durchsetzung der Richtlinien, Abläufe, Orientierungshilfen und Standards des Unternehmens
- Einhaltung der anwendbaren sozialen, steuerlichen und anderen gesetzlichen Anforderungen und Vorschriften
- IT-Sicherheitsmaßnahmen, um ein externes und / oder internes Eindringen in die Systeme zu verhindern
- Zugang zum Netzwerk des Unternehmens und IT-Support
- Die geschäftsbezogene Kommunikation
- Eine soziale Zusammenarbeit im Netzwerk des Unternehmens fördern
- Die Rechtsansprüche des Unternehmens bezogen auf Forderungen oder im Rahmen von auf das Geschäft bezogenen Rechtsstreitigkeiten bewahren oder verteidigen
- Verwaltung von Beschwerden und / oder Ansprüchen
- Verzeichnisse für persönliche Kontakte
- Versand von Unternehmenskommunikation

Es ist möglich, dass das Unternehmen zur Verhinderung, Aufdeckung und Ermittlung externer und/oder interner Angriffe auf die IT-Programme des Unternehmens personenbezogene Daten wie Log-Dateien oder IP-Adressen im gesetzlich zulässigen Rahmen verarbeitet und überträgt.

Weiterhin kann das Unternehmen personenbezogene Daten im Rahmen einer Ethik- und Compliance-Untersuchung verarbeiten. Dies schließt personenbezogene Daten zu der Person mit ein, die eine entsprechende Beschwerde vorgebracht hat (soweit diese Person ihre Identität zu erkennen gegeben hat). Ebenfalls darin eingeschlossen sind personenbezogene Daten zu Personen, die Gegenstand einer Beschwerde sind, sowie personenbezogene Daten von sonstigen Einzelpersonen, die uns bei einer Untersuchung unterstützen. Die Art der verarbeiteten personenbezogenen Daten hängt von der Art des erhaltenen Berichts ab und kann sensible personenbezogene Daten mit einschließen. Das Unternehmen wird solche personenbezogene Daten nur so lange vorhalten, wie dies für die Untersuchung der Ethik- und Compliance-Abteilung bzw. aus rechtlichen Gründen erforderlich ist.

7. Personenbezogene Daten übertragen und verarbeiten

Um Personenbezogene Daten zu Verarbeiten, ist es möglich, dass das Unternehmen diese im Verwaltungsprogramm der Personalabteilung oder in anderen computergestützten oder elektronischen Programmen oder Plattformen des Unternehmens speichert und diese lokal, regional oder weltweit - einschließlich in die USA - übertragen muss oder diese Daten anderen Venator-Unternehmen oder dritten Parteien gegenüber, die für das Unternehmen Services oder

Dienstleistungen bereitstellen, unter Berücksichtigung der erforderlichen Schutzmaßnahmen offenlegen muss.

Falls es für die Erreichung dieser Zwecke erforderlich ist, ist es möglich, dass die Personalabteilung, die Vorgesetzten oder Prüfer personenbezogene Daten im Rahmen ihrer Tätigkeit, ihrer Verantwortlichkeit oder ihrer zulässigen geschäftsbezogenen Aufgaben verarbeiten und übertragen. Darüber hinaus ist es möglich dass bestimmte Mitarbeiter des Unternehmen im Rahmen des Zulässigen in Bezug auf den geschäftsbezogenen Datenverkehr erforderliche Inhaltsanalyse durchführen und dabei Personenbezogene Daten Verarbeiten, sowie in Bezug auf die Überprüfung und Wartung der Betriebssysteme auf Personenbezogene Daten zugreifen müssen. Das Unternehmen unternimmt die nötigen Schritte, um zu gewährleisten, dass dieses Personal die Personenbezogenen Daten vertraulich behandelt.

Das Unternehmen verpflichtet sich, Personenbezogene Daten gemäß den Anwendbaren Gesetzen zu schützen. Das gilt unabhängig davon, ob die Empfänger innerhalb oder außerhalb der EU und der Schweiz ansässig sind. Das betrifft auch Länder, die keinen adäquaten Schutz in Bezug auf Personenbezogene Daten anbieten, oder Länder, die nicht über nationale Gesetze verfügen, die das gleiche Maß an Schutz von Personenbezogenen Daten sicherstellen. Jeder Transfer von personenbezogenen Daten in ein Land, das kein adäquates Maß an Datenschutz im Sinne der Anwendbaren Gesetze bereitstellt, erfolgt entweder auf Grundlage (i) der Zustimmung des Mitarbeiters, (ii) eines Datenverarbeitungsvertrages, (iii) des Privacy-Shield-Programms oder (iv) anderer entsprechender Schutzmaßnahmen gemäß den Anwendbaren Gesetzen oder dieser Unternehmensrichtlinie.

8. Mitteilung und Auswahl

Das Unternehmen wird personenbezogene Daten nur Zwecke verwenden, zu denen diese Personenbezogenen Daten ursprünglich erfasst wurden. Das Unternehmen wird keine Personenbezogenen Daten unter Änderung des Zweckes gegenüber Dritten offenlegen, außer die Betroffenen haben diesbezüglich ausdrücklich zugestimmt und dies ist gemäß den Privacy-Shield-Grundsätzen oder lokalen Standards gemäß den anwendbaren Gesetzen zulässig, oder für die Verarbeitung von Personenbezogenen Daten durch einen Auftragsverarbeiter, der dem Unternehmen hinreichende Gewährleistungen in Bezug auf technische und organisatorische Maßnahmen bereitstellt, die in Bezug auf den Schutz der personenbezogenen Daten unternommen wurden.

Die Verzeichnisse der Verarbeitungstätigkeiten gemäß den Anwendbaren Gesetzen, inklusive der Namen und Adressen von Auftragsverarbeitern, internen computergestützten oder elektronischen Programmen, die das Unternehmen nutzt, sowie Auflistungen von Ländern, in die personenbezogene Daten übertragen werden, können beim Privacy Team eingesehen werden.

9. Datensicherheit und -vollständigkeit

Das Unternehmen hat entsprechende technische und organisatorische Sicherheitsmaßnahmen zum Schutz der personenbezogenen Daten gegen Verlust, missbräuchliche Verwendung, nicht autorisierten Zugang, Offenlegung oder nicht autorisierte Änderung oder Vernichtung implementiert. Darüber hinaus sind die Mitarbeiter Gegenstand bestimmter Vertraulichkeitsverpflichtungen in Bezug auf die Handhabung und den Schutz von personenbezogenen Daten. Bei einem Verstoß gegen diese Verpflichtungen müssen Mitarbeiter mit disziplinarischen Maßnahmen bis hin zur Kündigung des Arbeitsverhältnisses rechnen.

Darüber hinaus unterhält das Unternehmen Verfahren, die dazu dienen, soweit entsprechend oder gemäß den Anwendbaren Gesetzen erforderlich, zu gewährleisten, dass personenbezogene Daten bezüglich ihres Verwendungszwecks zuverlässig sowie korrekt, vollständig und aktuell sind und

dass betroffene Personen ihr Recht auf Auskunft oder Löschung der personenbezogenen Daten ausüben kann. Wir möchten diesbezüglich betroffenen Personen darin bestärken, ihre personenbezogenen Daten ggf. zu aktualisieren, damit diese weiterhin korrekt, vollständig und aktuell sind. Das Unternehmen bewahrt personenbezogene Daten nur über den gemäß der „Document Retention Policy“ des Unternehmens erforderlichen oder mittels der Anwendbaren Gesetze zulässigen Zeitraum auf.

10. Rechte der Betroffenen

Mitarbeiter und andere Betroffene haben das Recht auf Auskunft über und Überprüfung ihrer Personenbezogenen Daten gemäß dem „globalen Datenschutzstandard“ und den Anwendbaren Gesetzen, um deren Korrektheit und ordnungsgemäße Verwendung zu verifizieren. Das kann beinhalten, Ermittlungen über die Zwecke der Verarbeitung, die Kategorien von diesbezüglichen personenbezogenen Daten und dritte Parteien oder Kategorien von dritten Parteien, denen gegenüber ihre personenbezogenen Daten offengelegt wurden, anzustellen. Mitarbeiter können hinsichtlich der durch das Unternehmen oder im Namen des Unternehmens gespeicherten Personenbezogenen Daten über ihre Person verlangen, diese Daten zu aktualisieren oder zu korrigieren, sofern dies angemessen oder erforderlich ist im Sinne der Anwendbaren Gesetze. Darüber hinaus können Mitarbeiter gemäß den Anwendbaren Gesetzen verlangen, dass ihre personenbezogenen Daten gesperrt oder gelöscht werden. Es ist jedoch in manchen Fällen, in denen der Aufwand oder die Kosten für die Bereitstellung des Zugangs bezüglich der Risiken des Datenschutzes des Mitarbeiters unverhältnismäßig wären, in denen gegen die Rechte anderer verstoßen würde, in denen vertrauliche geschäftliche Informationen oder Informationen über eine Nachfolgeplanung oder Reorganisation offengelegt würden oder in denen eine Complicance-, rechtliche oder regulative Angelegenheit, Funktion oder Privileg beeinträchtigt oder gefährdet würde, möglich, dass ein Zugang abgelehnt wird. Es ist möglich, dass das Unternehmen nach dem Verlassen des Unternehmen berechtigt oder gesetzlich verpflichtet ist, die personenbezogenen Daten eines Mitarbeiters in Bezug auf das Beschäftigungsverhältnis oder auf die gesetzlichen Pflichten des Unternehmens weiterhin zu verarbeiten.

Die Mitarbeiter schicken ihre Anfragen auf Auskunft, Änderung oder Löschung ihrer personenbezogenen Daten bitte schriftlich oder per E-Mail an das unten stehend angegebene Privacy Team oder ggf. an den lokalen Datenschutzbeauftragten.

11. Gemäß den Anwendbaren Gesetzen erforderliche oder zulässige Offenlegungen

Das Unternehmen kann unabhängig von jedweden sonstigen Bedingungen in dieser Richtlinie personenbezogene Daten im Kontext einer Veräußerung, Fusion, Transaktion oder Reorganisation, in die das gesamte Geschäft oder ein diesbezüglicher Teil involviert ist, oder im Rahmen von von externen Prüfern durchgeführten Audits, die erforderlich sind, um gesetzliche Anforderungen zu erfüllen, oder Fällen bei denen ohne eine Offenlegung die berechtigten Interessen des Unternehmens beeinträchtigen würde, oder für den Fall, dass dies gemäß den Anwendbaren Gesetzen erforderlich oder zulässig ist, offenlegen oder in anderer Form verarbeiten. Das Unternehmen wird – soweit irgend möglich - Maßnahmen der Pseudonymisierung und, Datenminimierung implementieren, um den erforderlichen Schutz von personenbezogenen Daten in diesen Arten an Transaktionen zu erreichen.

Darüber hinaus ist es möglich, dass das Unternehmen regelmäßig personenbezogene Daten Behörden und Regulierungsbehörden (z. B. Steuerbehörden), sozialen Organisationen (z. B. die Sozialversicherungsverwaltung), Anbietern von Personalzusatzleistungen (z. B. Krankenversicherer), dritten Parteien im Zusammenhang mit Reisen (z. B. um einen Flug, ein Hotelzimmer oder einen Mietwagen zu buchen), Gerichten und Behörden gegenüber offenlegt, soweit dies im Rahmen von rechtmäßigen Anfragen durch Behörden erforderlich ist, um nationale

Sicherheits- oder ordnungsrechtliche Anforderungen oder andere anwendbare gesetzliche Verpflichtungen gemäß den Anwendbaren Gesetzen zu erfüllen.

Das Unternehmen legt, soweit gemäß den Anwendbaren Gesetzen erforderlich, ohne vorherige schriftliche Einwilligung eines Mitarbeiters dessen personenbezogene Daten keiner dritten Partei gegenüber offen.

12. Personenbezogene Daten über Angehörige und verwandte Personen

Für den Fall, dass ein Mitarbeiter dem Unternehmen personenbezogene Daten seiner Angehörigen, Familienmitglieder und / oder verwandten Personen (z. B. bezüglich der Verwaltung von Zusatzleistungen und / oder als Notfallkontakt) bereitstellt, ist der Mitarbeiter dafür verantwortlich, diese Personen über die Verarbeitung ihrer personenbezogenen Daten durch das Unternehmen, über die Zwecke und die Art und Weise der Verarbeitung, wie sie in dieser Richtlinie angegeben sind, über ihr Recht auf Auskunft, Berichtigung und Löschung gemäß den Anwendbaren Gesetzen zu informieren. Ebenso ist der Mitarbeiter verpflichtet die Zustimmung zur Verarbeitung ihrer personenbezogenen Daten gemäß dieser Richtlinie (einschließlich des Transfers in Länder, die nicht das gleiche Maß an Schutz von personenbezogenen Daten wie ihr Herkunftsland bereitstellen) zu erwirken.

13. Anfragen von Mitarbeitern und Anliegen melden

Mitarbeiter können sich bei allen Themen und Fragen in Bezug auf die Anwendbaren Gesetze oder den Datenschutz beim Privacy Team oder ggf. dem lokalen Datenschutzbeauftragten informieren. Darüber hinaus können Anliegen oder Auskunftsanforderungen direkt an:

E-Mail: privacy@venatorcorp.com

Mitarbeiter mit Sitz in der EU finden zusätzliche Informationen zu dem ihnen zustehenden Beschwerderecht in der „Privacy Shield Policy“ des Unternehmens, die im Intranet (VenNet) nachgelesen werden kann.

Revisionshistorie des Dokuments

Richtlinien:	Datenschutz
Dokumentenreferenz:	PRIV-001
Ausstellungsdatum:	2018-006-06
Verzeichnisnummer:	11.1
Werte:	Vollständigkeit, null Nachteil, Teamwork, Innovation, Leistung

Política de Privacidad Global

1. Introducción

Venator Materials PLC, sus subsidiarias y compañías afiliadas ubicadas en todo el mundo (en conjunto, “Venator” o la “Compañía”) Procesan y Transfieren Datos Personales en la medida en que resulta necesario o pertinente para administrar su relación laboral o para cualquier otro propósito especificado, explícito y legítimo. En lo que a esto respecta y de acuerdo con esta Política de Privacidad Global ("Política"), la Compañía se esfuerza por cumplir con las Leyes aplicables en la medida que se apliquen a los asociados y otros individuos.

2. Alcance

La presente Política de Privacidad Global (“Política”) ofrece a los asociados información sobre cómo Procesa y Transfiere la Compañía Datos Personales a nivel local, regional e internacional, lo que incluye a título enunciativo las Transferencias a EE. UU. de acuerdo con las Leyes aplicables. El Equipo de Recursos Humanos, el Equipo de Privacidad o, si procede, el Delegado de Protección de Datos (“DPO”) local pueden facilitar más información sobre las políticas y los procedimientos de la Compañía relacionados con los Datos Personales.

3. Definiciones

Leyes aplicables

Los principios de las leyes de protección de datos que establece el Reglamento General de Protección de Datos de la Unión Europea (“RGPD”), los principios del Escudo de Privacidad o la legislación local en materia de protección de datos, la normativa que sea más estricta.

Datos Personales

Toda información relacionada con una persona física identificada o identificable. Una persona identificable es aquella que puede ser identificada, de forma directa o indirecta, en particular por referencia a un identificador tal como un nombre, un número de identificación, información de ubicación, un identificador en línea o a uno o más factores específicos relativos a su identidad física, psicológica, genética, mental, económica, cultural o social. En la Sección 5 a continuación se incluyen las categorías de Datos Personales obtenidos y Procesados por la Compañía o un tercero.

Controlador de Datos

La entidad que de forma independiente o en conjunto con otros determina los propósitos y los medios del Procesamiento de Datos Personales.

Procesador de Datos

La entidad que Procesa los Datos Personales en nombre del Controlador.

Procesar/Procesado/Procesamiento

Una operación o conjunto de operaciones que se realiza con respecto a Datos Personales, ya sea mediante medios automáticos o no, tales como recopilación, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación mediante

transmisión, difusión o de otra forma puesta a disposición, cotejo o combinación, restricción, eliminación o destrucción.

Transferir/Transferido/Transferencia

Cuando una parte o la Compañía pone Datos Personales a disposición de otra parte o de la Compañía por cualquier medio.

4. Declaración del Escudo de Privacidad

Con respecto a los Datos Personales de los asociados, la Compañía reconoce que existe un régimen de protección de datos “general” con arreglo a las Leyes aplicables. Las Leyes aplicables generalmente restringen la Transferencia de Datos Personales de los asociados de la UE o Suiza a EE. UU., a menos que exista "protección adecuada" para dichos Datos Personales cuando se reciban en los EE. UU. A los efectos de cumplir con esta restricción, la Compañía se adhiere a los principios del Escudo de Privacidad de los EE.UU./UE y EE. UU./Suiza publicados por la Comisión Federal de Comercio de los EE. UU. con respecto a los Datos Personales que la Compañía recibe en los EE. UU. Se puede consultar más información sobre el Escudo de Privacidad en la Política del Escudo de Privacidad de la Compañía que se encuentra en la página de la intranet del RGPD de VenNet o en el sitio web de la Comisión Federal de Comercio de EE. UU., en https://www.privacyshield.gov/welcome.

5. Definición y recopilación de Datos Personales

Los tipos de Datos Personales que la Compañía puede recibir, Procesar y Transferir a nivel local, regional y mundial, incluyendo Transferencias a EE. UU., o divulgar a otras compañías de Venator u organizaciones de terceros que suministren servicios de administración o de otro tipo a la Compañía, están divididos en Categorías de Datos Personales. Las Categorías de Datos Personales desencadenan mayores requisitos de restricción, basados en la importancia de los Datos Personales, para privilegios de acceso interno y protecciones de manejo de datos físicos requeridos por asociados cuyas tareas empresariales válidas incluyen el manejo de Datos Personales.Estas Categorías de Datos Personales se diseñaron para (i) ayudar a los asociados a reconocer rápidamente la importancia relativa de dichos Datos Personales con respecto a los derechos personales de un individuo para el propósito de manejo y protección interna y externa y (ii) mejorar la formación de conocimiento de lo propósitos permisibles y limitados de acceso, uso y divulgación para cada Categoría de Datos Personales, con el fin de protegerla de hurto, puesta en riesgo, uso inapropiado y visualización por asociados no autorizados u otros individuos.

Las Categorías de Datos Personales son las siguientes:

Categoría 1 (verde) – Información de identificación comercial y de contacto del individuo

El nombre del individuo y la información de contacto laboral, como por ejemplo número de teléfono laboral, dirección comercial y dirección de correo electrónico;

Categoría 2 (amarillo) - Datos Personales creados por la Compañía

Información relacionada con el trabajo y el salario como, por ejemplo, información de compensaciones, bonificaciones e incentivos, información general con respecto a prestaciones, pensiones por jubilación, desempeño, cumplimiento de las políticas, procedimientos, normas y pautas sobre medioambiente, seguridad e higiene e investigaciones relacionadas, capacitación y desarrollo y cumplimiento de las políticas, procedimientos, normas y pautas de la Compañía e investigaciones relacionadas;

Categoría 3 (naranja) – Datos Personales provistos por el individuo

Información relacionada con información de ubicación o identificador en línea tal como dirección personal, número de teléfono personal y del domicilio particular, conocimientos laborales y educativos, viajes y gastos comerciales e imagen;

Categoría 4 (rojo) - Datos Personales que pueden considerarse importantes

Según las Leyes aplicables, los Datos Personales que pueden ser considerados Datos Personales importantes, los cuales incluyen información de identificación emitida por el gobierno, raza u origen étnico, creencias religiosas, información genética, enfermedad física o de salud mental o discapacidad, orientación sexual, información bancaria personal o de tarjetas de pago, afiliación sindical, antecedentes criminales y cualquier castigo recibido por un delito comprobado o cualesquiera otros datos que impidan de forma grave los derechos personales del individuo afectado.

Además, si un asociado necesita obtener un visado para trabajar en los EE. UU. u otro lugar, es posible que la Compañía le solicite al asociado y a los familiares que lo acompañen que proporcionen Datos Personales adicionales o información familiar a la Compañía para ayudarlo con las solicitudes de visado. También es posible que la Compañía reciba determinada información con respecto al cónyuge del asociado, familiares u otras personas dependientes como contactos de emergencia (si los proporciona de forma voluntaria) y para propósitos de administración de prestaciones.

La Compañía recibe Datos Personales que son "importantes" según el significado recogido por las Leyes aplicables y en la medida en que estas lo permitan, por ejemplo si es necesario para la ejecución del empleo o la relación contractual. En particular, la Compañía puede recibir y Procesar Datos Personales que son importantes en relación con la salud y/o discapacidades del asociado para los propósitos empresariales de la administración de prestaciones de salud, programas de controles médicos, administración de bajas o alojamiento por obligaciones laborales.

Los Datos Personales pueden ser recopilados con anterioridad al comienzo de la relación laboral, como por ejemplo durante el proceso de reclutamiento, y también a lo largo de la relación laboral del asociado, ya sea por medios electrónicos y/o en papel.

6. Usos de los Datos Personales por la Compañía

La Compañía puede Procesar y Transferir Datos Personales de forma local, regional y mundial, incluyendo EE. UU., en relación con un asociado para fines tales como los que se mencionan a continuación, según lo permitan las Leyes aplicables:

- Contactos de emergencia
- Consideración de contratación o ascenso
- Administración de personal y obligaciones laborales
- Gestión de desempeño y capacitación y desarrollo
- Administración de licencias
- Facilitar el procesamiento de informes de gastos de viajes
- Administración de compensación, bonificaciones, pensiones, prestaciones y programas de incentivos
- Administración de prestaciones de salud, compensación de los trabajadores y programas de controles médicos
- Administración de programas relacionados con la compensación ejecutiva
- Gestión del flujo de trabajo y continuidad
- Preparación de presupuestos y planificación

- Planificación de sucesión
- Venta, fusión o reorganización empresarial
- Encuestas personales relacionadas con la Compañía
- Procesamiento de solicitudes de visado y permisos de trabajo
- Cumplimiento y consideraciones legales que requieren investigación, auditoría, y cumplimiento de las políticas, procedimientos, pautas y normas de la Compañía
- Cumplimiento con requisitos y regulaciones sociales e impositivos aplicables y con otros requisitos y regulaciones legales
- Medidas de seguridad de TI para evitar intrusiones externas y/o internas
- Acceso a la red de la Compañía y soporte de TI
- Comunicaciones empresariales
- Facilitar la colaboración social en la red de la Compañía
- Conservar o defender los derechos legales de la Compañía después de demandas o durante litigios empresariales
- Administración de quejas y/o reclamaciones
- Directorios de contactos personales
- Envío de comunicaciones de la Compañía

Para la prevención, detección o investigación de intrusiones externas y/o internas en los sistemas de TI de la Compañía, esta podrá Procesar y Transferir Datos Personales tales como los archivos de registro o las direcciones IP, en la medida en que lo permitan las Leyes aplicables.

Además, la Compañía podría Procesar Datos Personales como parte de cualquier investigación de Ética y Cumplimiento. Esto incluye los Datos Personales acerca de la persona que realiza la queja (en la medida en que la persona se haya identificado), los Datos Personales acerca de cualquier individuo que sea el objeto de la queja y los Datos Personales de cualquier otro individuo que nos ayude en la investigación de la Compañía. La naturaleza de los Datos Personales Procesados depende de la naturaleza del informe recibido y puede incluir Datos Personales confidenciales. La Compañía solo retendrá dichos Datos Personales por el tiempo que sea relevante para la investigación de Ética y Cumplimiento o necesario por motivos legales.

7. Transferencias y Procesamiento de Datos Personales

A fin de Procesar Datos Personales para estos propósitos, es posible que sea necesario que la Compañía almacene en su sistema de información de Recursos Humanos u otros sistemas o plataformas electrónicos o computarizados de la Compañía y que realicemos la Transferencia a nivel local, regional o mundial, incluyendo EE. UU., o que la divulguemos a otras compañías de Venator u organizaciones de terceros que suministren servicios de administración o de otro tipo a la Compañía, con sujeción a las protecciones apropiadas.

Según sea necesario, en relación con estos propósitos, el Equipo de Recursos Humanos, gerentes o supervisores funcionales pueden Procesar y Transferir Datos Personales relacionados con sus responsabilidades laborales y tareas empresariales válidas relacionadas. Si las Leyes aplicables lo permiten, ciertos asociados dentro de la Compañía también podrán tener acceso a Datos Personales relacionados con el tráfico de TI y análisis de contenido relacionado con los negocios y monitoreo y mantenimiento de sistemas operativos. La Compañía toma las medidas necesarias diseñadas para garantizar que ese personal mantenga la confidencialidad con respecto a los Datos Personales.

El objetivo de la Compañía es proteger los Datos Personales de acuerdo con las Leyes aplicables sin tener en cuenta si los beneficiarios se encuentran dentro o fuera de la UE o Suiza, incluyendo países que puedan no ofrecer el mismo nivel de protección de Datos Personales o países que no posean leyes que ofrezcan el mismo nivel de protección de Datos Personales. Toda Transferencia de Datos Personales a un país que no ofrezca un nivel adecuado de protección de datos, según el

significado que estipulan las Leyes aplicables, se realizará en base a (i) consentimiento del asociado, (ii) Contrato de Transferencia de Datos, (iii) el Programa de Escudo de Privacidad u (iv) otras medidas de protección apropiadas según las Leyes aplicables o la política de la Compañía.

8. Aviso y elección

La intención de la Compañía es utilizar los Datos Personales para los propósitos para los que originalmente se recopilaron y no divulgarla a un tercero para un propósito incompatible, excepto que los individuos afectados otorguen el consentimiento que corresponde y esté permitido bajo los principios de Escudo de Privacidad o las normas locales de conformidad con las Leyes aplicables, o para el Procesamiento de Datos Personales por parte de un Procesador externo que proporcione a la Compañía las garantías suficientes en relación con las medidas técnicas y organizacionales que se toman en relación con la protección de los Datos Personales.

Cualquier listado exigido por las Leyes aplicables de los nombres y las direcciones de terceros Procesadores y sistemas electrónicos internos electrónicos o computarizados utilizados por la Compañía, así como cualquier listado exigido de los países a los que se Transfieren Datos Personales puede solicitarse al Equipo de Privacidad.

9. Seguridad e integridad de los datos

La Compañía ha implementado medidas de seguridad técnicas y organizativas apropiadas para proteger los Datos Personales de pérdida, uso inapropiado, acceso no autorizado, divulgación o alteración o destrucción no autorizados. Los asociados están sujetos a ciertas obligaciones de confidencialidad relacionadas con el manejo y la protección de Datos Personales y pueden ser sancionados o despedidos si no cumplen con estas obligaciones.

La Compañía también cuenta además con procedimientos diseñados para ayudar a garantizar, en la medida que sea apropiado o requerido por las Leyes aplicables, que los Datos Personales sean confiables para el uso pretendido y precisos, completos y actuales y que el individuo pueda ejercitar sus derechos para acceder a los Datos Personales o suprimirlos. Con respecto a esto, se invita al individuo a que actualice sus Datos Personales cuando sea necesario para que sean precisos, estén completos y sean actuales. La Compañía solo conserva los Datos Personales durante el plazo que exige el Procedimiento de Retención de Documentos de la Compañía o que permitan las Leyes aplicables.

10. Acceso a Datos Personales

Los asociados u otros individuos pueden tener derecho al acceso y revisión de sus propios Datos Personales de acuerdo con el Procedimiento de Privacidad Global y las Leyes locales aplicables para verificar su precisión y usos legítimos, lo que puede incluir consultar sobre los propósitos del Procesamiento, las categorías de Datos Personales en cuestión y los terceros o categorías de terceros a quienes se divulgan sus Datos Personales. Cuando sea apropiado según las Leyes aplicables o estas así lo requieran, con respecto a los Datos Personales conservados por o en nombre de la Compañía, un asociado podrá actualizar o corregir sus Datos Personales incorrectos. Con sujeción a las Leyes aplicables, un asociado también podrá solicitar que sus Datos Personales sean bloqueados o eliminados. Sin embargo, en determinadas ocasiones, puede negarse el acceso cuando la carga o gasto de proporcionar acceso sean desproporcionados con respecto a los riesgos para la privacidad del asociado, cuando se vulnerarían los derechos de otros, cuando sería revelada información comercial confidencial o planificación de sucesión o información de reorganización o cuando un asunto de cumplimiento, legal o reglamentario, función o privilegio se vería perjudicado o menoscabado. Después de dejar la Compañía, esta podría tener derecho o estar obligada por ley a continuar Procesando los Datos

Personales de un asociado con respecto a la relación laboral o las responsabilidades legales de la Compañía.

Un asociado debería enviar solicitudes de acceso, modificación o supresión de sus Datos Personales, por escrito o por correo electrónico, al Equipo de Privacidad, identificado a continuación, o al Delegado de Protección de Datos.

11. Divulgaciones requeridas o permitidas por las Leyes aplicables

Independientemente de las disposiciones de esta Política, la Compañía puede divulgar o Procesar de otra manera Datos Personales en el contexto de venta, fusión, transacción o reorganización que involucre a toda la Compañía o una parte de esta o con el propósito de auditorías llevadas a cabo por auditores externos, según sea necesario para satisfacer requisitos reglamentarios, o en otras circunstancias en las que la no divulgación perjudicaría los intereses legítimos de la Compañía, o según lo requieran o permitan las Leyes aplicables. La Compañía tiene intención de aplicar medidas apropiadas, tales como la seudonimización y la reducción de los datos al mínimo, para proteger debidamente los Datos Personales en estos tipos de transacciones.

La Compañía también podría divulgar Datos Personales a agencias y reguladores gubernamentales (por ejemplo, autoridades impositivas), organizaciones sociales (por ejemplo, la administración de seguridad social), proveedores de prestaciones de Recursos Humanos (por ejemplo, aseguradoras de salud), terceros relacionados con viajes (por ejemplo, para reservar un vuelo, habitación de hotel o alquilar un coche), cortes y otros tribunales y autoridades gubernamentales o en la medida que lo requieran solicitudes legítimas de autoridades públicas para cumplir con los requisitos de cumplimiento y seguridad nacional u otras obligaciones legales, según las Leyes aplicables.

Si las Leyes aplicables lo solicitan, la Compañía no divulgará los Datos Personales de un asociado a ningún tercero sin haber obtenido su consentimiento por escrito.

12. Datos Personales sobre dependientes y personas relacionadas

Si un asociado ofrece a la Compañía Datos Personales sobre sus dependientes, familiares y/o personas relacionadas (por ejemplo, para la administración de prestaciones y/o contactos de emergencia), el asociado es responsable de informarles a dichos individuos que la Compañía Procesará sus Datos Personales para los propósitos que se describen en esta Política y de la forma en la que se describen, sus derechos de acceso, corrección y eliminación conforme a las Leyes aplicables, así como también de obtener el consentimiento, cuando sea necesario, para el Procesamiento (incluyendo la Transferencia a países que podrían no ofrecer el mismo nivel de protección de Datos Personales que su país de origen) de sus Datos Personales como se establece en esta Política.

13. Consultas de asociados e informar inquietudes

Un asociado puede informarse de cualquier tema relativo a las Leyes aplicables acudiendo al Equipo de Privacidad o al Delegado de Protección de Datos local, en su caso. Pueden enviarse las consultas o solicitudes de acceso también:

E-mail: privacy@venatorcorp.com

Para los asociados en la UE, se proporciona información adicional sobre el proceso de quejas relativo a los asociados de la UE en la Política de Escudo de Privacidad de la Compañía, que se puede encontrar en el sitio de la Intranet de la Compañía.

Document Revision History

Política:	Privacidad
Referencia del documento:	PRIV-001
Fecha de emisión:	2018-06-06
Número de índice:	11.1
Valores:	Integridad, Daño cero, Trabajo en equipo, Innovación, Rendimiento

1. Johdanto

Venator Materials PLC eri puolilla maailmaa toimivine tytäryhtiöineen ja sivuliikkeineen (joita kutsutaan kollektiivisesti nimillä ”Venator” tai ”yritys”) käsittelee ja siirtää henkilötietoja siinä määrin kuin se on välttämätöntä tai tarkoituksenmukaista työsuhteesi hallinnoimiseen tai muuhun määritettyyn, nimenomaiseen ja lainmukaiseen tarkoitukseen. Tähän liittyen ja tätä yleistä tietosuojakäytäntöä (”käytäntö”) noudattaen yritys pyrkii noudattamaan sovellettavia lakeja siltä osin, kuin niitä sovelletaan henkilöstöön ja muihin henkilöihin.

2. Laajuus

Tämä yleinen tietosuojakäytäntö (”käytäntö”) sisältää henkilöstölle suunnattuja tietoja siitä, kuinka yritys käsittelee ja siirtää henkilötietoja paikallisesti, alueellisesti ja maailmanlaajuisesti, mukaan lukien tietojen siirto Yhdysvaltoihin sovellettavien lakien mukaisesti. Yrityksen käytännöistä ja henkilötietojen käsittelyyn liittyvistä menetelmistä saa tarvittaessa lisätietoja HR-tiimiltä, tietosuojasta vastaavalta tiimiltä tai paikalliselta tietosuojavastaavalta (Data Protection Officer, DPO).

3. Määritelmät

Sovellettavat lait

Tietosuojalainsäädäntöä koskevat periaatteet määritetään eurooppalaisessa tietosuoja-asetuksessa (General Data Protection Regulation, GDPR), yksityisyyden suojaa koskevissa periaatteissa tai paikallisessa tietosuojalainsäädännössä sen mukaan, mikä niistä on tiukin.

Henkilötiedot

Tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä koskevat tiedot. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. Yrityksen tai kolmannen osapuolen keräämien ja käsittelemien henkilötietojen ryhmät määritetään alla kohdassa 5.

Rekisterinpitäjä

Taho, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Tietojen käsittelijä

Taho, joka käsittelee henkilötietoja rekisterinpitäjän puolesta.

Käsittely/käsitteleminen/käsitelty

Käsittelytoimi tai käsittelytoimet, joissa kohteena ovat henkilötiedot, joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku, kysely, käyttö,

tietojen luovuttaminen siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittaminen tai yhdistäminen, rajoittaminen, poistaminen tai tuhoaminen.

Siirto/siirtäminen/siirretty

Kun toinen taho tai yritys asettaa henkilötietoja toisen osapuolen saataville, tavasta riippumatta.

4. Yksityisyyden suojaa koskeva lausunto

Yritys noudattaa henkilöstönsä henkilötietojen suojaamisessa kattavaa tietosuojajärjestelmää sovellettavien lakien mukaisesti. Sovellettavat lait rajoittavat yleisesti henkilöstön henkilötietojen siirtoa EU:sta tai Sveitsistä Yhdysvaltoihin, jollei kyseisiä henkilötietoja suojata Yhdysvalloissa vastaanotettaessa ”riittävin suojatoimin”. Yritys noudattaa tätä rajoitusta Yhdysvaltoihin saapuvien henkilötietojen osalta noudattamalla Yhdysvaltain ja EU:n sekä Yhdysvaltain ja Sveitsin välisiä yksityisyyden suojaa koskevia periaatteita, jotka Yhdysvaltain kuluttajansuojaa valvova elin Federal Trade Commission on julkaissut. Lisätietoa yksityisyyden suojaa koskevista periaatteista on yrityksen tietosuojakäytännössä, joka löytyy VenNet-järjestelmän yleistä tietosuoja-asetusta koskevalta GDPR-intranet-sivulta tai Yhdysvaltain Federal Trade Commissionin verkkosivuilta osoitteessa https://www.privacyshield.gov/welcome.

5. Henkilötietojen määritelmä ja kerättävät henkilötiedot

Henkilötiedot, joita yritys voi vastaanottaa, käsitellä ja siirtää paikallisesti ja maailmanlaajuisesti, mukaan lukien siirrot Yhdysvaltoihin, tai luovuttaa muille Venator-yrityksille tai yritykselle hallinto- tai muita palveluita tuottaville kolmannen osapuolen organisaatioille on jaoteltu henkilötietoryhmiin. Henkilötietoryhmille on asetettu tiukempia rajoituksia henkilötietojen arkaluonteisuuden takia. Rajoitukset koskevat sisäisiä käyttöoikeuksia ja tietojen fyysisiä käsittelytoimia koskevia suojatoimia, joita edellytetään niiltä henkilöstöön kuuluvilta, joiden työtehtäviin kuuluu henkilötietojen käsittelyä. Näiden henkilötietoryhmien tarkoitus on (i) auttaa henkilöstöä tunnistamaan arkaluontoiset henkilötiedot nopeasti ja tuntemaan yksilön oikeudet, jotka liittyvät henkilötietojen suojaukseen ja käsittelyyn yrityksen sisällä tai ulkopuolella (ii) informoida kunkin henkilötietoryhmän saantiin, käyttöön ja luovuttamiseen liittyvistä sallituista ja rajoitetuista toimenpiteistä, joiden avulla henkilötietoja suojataan varkaudelta, tietoturvaloukkaukselta, väärinkäytöltä ja luvattomalta käytöltä valtuuttamattomien työntekijöiden tai muiden henkilöiden toimesta.

Henkilötietoryhmät:

Luokka 1 (vihreä) - Henkilön yhteystiedot ja yritykseen liittyvät tiedot

Henkilön nimi ja työyhteystiedot, kuten työpuhelinnumero(t), yrityksen osoite ja sähköpostiosoite;

Luokka 2 (keltainen) - Yrityksen luomat henkilötiedot

Työsuhteeseen ja palkkaukseen liittyvät tiedot, kuten palkkatiedot; bonukset ja kannustepalkkio; etuja koskevat yleistiedot; eläketiedot; työtulokset; EHS-periaatteiden, menettelytapojen, standardien ja ohjeiden noudattaminen sekä muut tutkimukset; koulutus ja kehitys sekä yrityksen periaatteiden, menetelmien, standardien ja ohjeiden noudattaminen ja muut tutkimukset;

Luokka 3 (oranssi) - Henkilön itsensä antamat henkilötiedot

Sijaintitieto tai verkkotunnistetieto, kuten kotiosoite; kotipuhelin ja muut henkilökohtaiset puhelinnumerot; sähköposti- ja IP-osoitteet; työhistoria ja koulutustausta; Työmatkakulut ja muut kulut; ja valokuva;

Luokka 4 (punainen) - Henkilötiedot, jotka voidaan katsoa arkaluonteisiksi

Sovellettavien lakien mukaan arkaluonteisiksi henkilötiedoiksi voidaan katsoa mm. valtion myöntämät henkilötunnukset, rotu tai etninen alkuperä; uskonto; geneettiset tiedot; fyysinen tai henkinen terveys tai vamma; seksuaalinen suuntautuminen; henkilökohtaiset pankkitiedot tai maksukorttitiedot; ammattiliiton jäsenyys; rikosrekisteriote sekä rikostuomiot tai muut henkilötiedot, jotka haittaavat vakavasti kyseisen henkilön oikeuksia.

Jos henkilöstön jäsenen on hankittava Yhdysvaltoihin tai muuhun maahan työviisumi, yrityksellä on oikeus pyytää henkilöstön jäsentä tai hänen mukanaan muuttavaa perheenjäsentä toimittamaan yritykselle viisumihakemuksessa tarvittavia muita henkilötietoja tai perhetietoja. Yritys saattaa myös saada haltuunsa tiettyjä tietoja henkilöstön jäsenen puolisosta, perheenjäsenistä tai muista hätäyhteyshenkilöistä (mikäli nämä tiedot annetaan vapaaehtoisesti) sekä tukiin tai etuihin liittyviin hallintotarkoituksiin.

Yritys vastaanottaa määrityksen ja sovellettavien lakien ”arkaluonteisia” henkilötietoja esimerkiksi silloin, kun niitä tarvitaan työsuhteen tai sopimussuhteen täytäntöönpanossa. Yritys voi etenkin vastaanottaa ja käsitellä henkilöstön jäsenen terveyteen ja/tai vammoihin liittyviä arkaluonteisia henkilötietoja, jos niitä tarvitaan työterveyshoidon, terveyden seurantaohjelmien tai perhevapaiden hallintaan tai työtehtävien mukauttamiseen.

Henkilötietoja voidaan kerätä ennen työsuhteen alkamista esimerkiksi rekrytointiprosessin aikana ja koko henkilöstön jäsenen työsuhteen ajan joko verkon kautta ja/tai kirjallisesti.

6. Tavat, joilla yritys käyttää henkilötietoja

Yhtiö voi käsitellä ja siirtää henkilöstönsä jäsenen henkilötietoja paikallisesti, alueellisesti ja maailmanlaajuisesti, mukaan lukien Yhdysvalloissa sovellettavien lakien mukaisesti esimerkiksi seuraavasti:

- Yhteyshenkilöt hätätapauksessa
- Henkilöä harkitaan tiettyyn työtehtävään tai ylennettäväksi
- Henkilöstöhallinto ja työtehtävien hallinta
- Työsuoritusten hallinta, koulutus ja kehittämistyö
- Perhevapaiden hallinta
- Matkustamisen helpottaminen ja kulukorvausraporttien käsittely
- Korvauksiin, bonuksiin, eläkkeeseen, etuihin ja kannustepalkkioihin liittyvät ohjelmat
- Työterveysetuihin, työntekijöille maksettaviin korvauksiin ja terveydentilan seurantaan liittyvät ohjelmat
- Johtotason palkkio-ohjelmien hallinta
- Työnkulun hallinta ja jatkuvuus
- Budjetointi ja suunnittelu
- Henkilöstösuunnittelu
- Yrityksen myynti, sulautuminen tai uudelleenjärjestelyt
- Yritystoimintaan liittyvät henkilöstökyselyt
- Viisumihakemusten ja työlupien käsittely
- Vaatimustenmukaisuus ja oikeudelliset näkökohdat, jotka edellyttävät yrityksen toimintatapojen, käytäntöjen, ohjeiden ja standardien tutkintaa, auditointia ja käyttöönottoa
- Sovellettavien yhteiskunnallisten, veroihin liittyvien ja muiden lainmukaisten vaatimusten ja määräysten noudattaminen
- IT-tietoturvatoimet, joilla estetään yrityksen ulkoa ja/tai sisältä tehtävät tietomurrot
- Yritysverkon käyttöoikeus ja IT-tuki
- Yritysviestintä

- Yhteisöllisen toiminnan helpottaminen yritysverkossa
- Yrityksen laillisten oikeuksien säilyttäminen tai puolustaminen vaatimusten yhteydessä tai yritystoimintaan liittyvän oikeudenkäynnin aikana
- Kurinpidollisten toimien ja/tai vaatimusten hallinta
- Henkilökohtaiset yhteystietojen hakemistot
- Yritysviestinnän postitus

Estääkseen, havaitakseen ja selvittääkseen yritykseen ulkoa ja/tai sisältä kohdistuvat IT-järjestelmien tietomurrot yrityksellä on oikeus käsitellä ja siirtää henkilötietoja, kuten lokitiedostoja ja IP-osoitteita sovellettavien lakien sallimassa määrin.

Lisäksi yritys voi käsitellä henkilötietoja osana eettisyyden ja vaatimustenmukaisuuden tutkimusta. Näihin lukeutuvat valituksen tehneen henkilön henkilötiedot (siinä määrin, kun henkilö on ilmoittanut niistä), sen henkilön henkilötiedot, jota valitus koskee, sekä kaikkien niiden henkilöiden henkilötiedot, jotka auttavat meitä yrityksen tutkimuksissa. Henkilötietojen luonne riippuu saadun raportin luonteesta, ja niihin saattavat lukeutua arkaluontoiset henkilötiedot. Yritys säilyttää sellaisia henkilötietoja niin kauan, kun ne ovat olennaisia eettisyyden ja vaatimustenmukaisuuden tutkimukselle tai laillisista syistä.

7. Henkilötietojen siirrot ja käsittely

Henkilötietojen käsittelyä varten yrityksen voi olla tarpeen tallentaa tiedot yrityksen henkilöstöhallinnon tietojärjestelmään tai yrityksen muuhun IT- tai sähköiseen järjestelmään tai muille alustoille ja siirtää niitä paikallisesti, alueellisesti ja maailmanlaajuisesti, mukaan lukien Yhdysvaltoihin, tai luovuttaa niitä asianmukaisia suojatoimia noudattaen muille Venatoriin kuuluville yrityksille tai kolmansille osapuolille, jotka toimittavat hallinto- tai muita palveluita yritykselle.

Tarvittaessa henkilöstöhallinnon tiimi, toiminnalliset päälliköt ja esimiehet voivat näissä tarkoituksissa käsitellä ja siirtää henkilötietoja vastuualueisiinsa liittyen ja yritystoimintaan liittyvissä tehtävissään. Sovellettavien lakien salliessa myös tietyillä yrityksen henkilöstön jäsenillä on oikeus päästä henkilötietoihin heidän suorittaessaan tehtäviä, jotka liittyvät yrityskohtaiseen tietoliikenteeseen ja sisältöanalyysiin sekä käyttöjärjestelmien valvontaan ja huoltoon. Yritys ryhtyy tarvittaviin toimenpiteisiin, joiden avulla varmistetaan, että nämä henkilöstön jäsenet käsittelevät henkilötietoja luottamuksellisesti.

Yhtiö aikoo suojella henkilötietoja sovellettavien lakien mukaisesti riippumatta siitä, ovatko vastaanottajat EU:n tai Sveitsin alueella tai niiden ulkopuolella tai maissa, joissa henkilötietoja ei välttämättä suojata yhtä tiukin kriteerein tai joissa henkilötietojen suojaa koskeva lainsäädäntö ei ole yhtä tiukka. Henkilötietojen siirto maahan, jossa henkilötietojen tietosuojan taso ei ole riittävä sovellettavien lakien tarkoittamalla tavalla tehdään aina (i) henkilöstön jäsenen luvalla, (ii) tietojen siirrosta tehdyn sopimuksen perusteella, (iii) yksityisyyden suojaa koskevan lausunnon mukaisesti, tai (iv) muuta vastaavaa suojatoimea noudattaen sovellettavan lainsäädännön tai yrityksen tietosuojaperiaatteiden mukaisesti.

8. Ilmoitus ja oikeudet

Yhtiö aikoo käyttää henkilötietoja niihin tarkoituksiin, joihin henkilötiedot alun perin kerättiin. Yhtiö ei aio luovuttaa henkilötietoja kolmansille osapuolille muihin tarkoituksiin, paitsi yksityisyyden suojaa koskevan lausunnon tai paikallisten lakien mukaisesti kyseisen henkilön antamalla luvalla, tai luovuttaakseen henkilötiedot käsiteltäväksi kolmannelle osapuolelle, joka toimittaa yritykselle riittävät takuut siitä, että henkilötiedot suojataan teknisin ja organisatorisin toimenpitein.

Tietosuojasta vastaavalta tiimiltä saa sovellettavien lakien edellyttämän luettelon yrityksen käyttämien kolmannen osapuolen käsittelijöiden ja sisäisten IT- tai sähköisten järjestelmien nimistä

ja osoitteista sekä sovellettavien lakien edellyttämän luettelon maista, joihin henkilötietoja siirretään.

9. Tietoturva ja tietojen eheys

Yhtiö on ottanut käyttöön asianmukaiset tekniset ja organisatoriset turvatoimet, joilla henkilötiedot suojataan häviämiseltä, väärinkäytöltä, luvattomalta käytöltä, luovuttamiselta tai luvattomalta muuttamiselta tai tuhoamiselta. Henkilöstön jäsenillä on lisäksi henkilötietojen luottamuksellista käsittelyä ja suojaamista koskevia velvoitteita, ja vaatimusten laiminlyönti voi johtaa kurinpidollisiin toimiin tai työsuhteen irtisanomiseen.

Yhtiö ylläpitää ohjeita, joiden avulla voidaan sovellettavien lakien suosittelemalla tai edellyttämällä tavalla varmistaa, että henkilötietoihin voidaan luottaa käyttötarkoituksessaan ja että ne ovat tarkkoja, täydellisiä ja ajantasaisia, ja että henkilö voi oikeutensa mukaisesti saada henkilötietonsa nähtäväksi tai pyytää niiden poistamista. Tämän vuoksi suosittelemme, että jokaista kannustetaan päivittämään omat henkilötietonsa. Näin ne pysyvät tarkkoina, täydellisinä ja ajantasaisina. Yritys säilyttää henkilötietoja vain niin kauan kuin yrityksen asiakirjojen säilyttämistä koskevassa periaatteessa edellytetään tai sovellettavissa laeissa sallitaan.

10. Pääsy henkilötietoihin

Henkilöstön jäsenillä ja muilla henkilöillä on oikeus päästä näkemään omat henkilötietonsa yleisen tietosuojakäytännön ja sovellettavien lakien mukaisesti, varmistaakseen tietojen tarkkuuden ja lainmukaisen käytön. Tämä voi sisältää oikeuden tiedustella henkilötietojen käsittelytarkoitusta, henkilötietoryhmiä sekä kolmansia osapuolia tai niiden ryhmiä, joille omia henkilötietoja on luovutettu. Mikäli sovellettavissa laeissa näin suositellaan tai edellytetään, henkilöstön jäsenellä on oikeus päivittää tai korjata yrityksen tai sen toimeksiannosta toimivan tahon hallussa olevia virheellisiä henkilötietojaan. Sovellettavien lakien mukaisesti henkilöstön jäsenellä on myös oikeus pyytää omien henkilötietojensa käytön estämistä tai poistamista. Joissakin tapauksissa pääsy henkilötietoihin saatetaan kuitenkin estää, mikäli pääsyn mahdollistamisesta koituisi suhteetonta vaivaa tai suhteettomia kustannuksia verrattuna henkilöstön jäsenen yksityisyydensuojan riskeihin, mikäli se rikkoisi muiden oikeuksia, mikäli sen yhteydessä paljastuisi luottamuksellista liiketoimintatietoa tai henkilöstösuunnittelun yksityiskohtia tai organisaation uudelleenjärjestelyjä koskevia tietoja tai mikäli se saattaisi haitata tai vaarantaa säännönmukaista toimintaa, lainsäädäntöön tai asetuksiin liittyvää asiaa, tehtävää tai etua. Kun henkilöstön jäsen on lähtenyt yrityksen palveluksesta, yrityksellä on oikeus tai sillä voi olla lainmukainen velvollisuus jatkaa hänen henkilötietojensa käsittelyä työsuhteeseen tai yrityksen lakisääteisiin velvollisuuksiin liittyen.

Jos henkilöstön jäsen haluaa pyytää pääsyä henkilötietoihinsa tai henkilötietojensa täydentämistä tai poistamista, pyyntö on lähetettävä kirjallisesti tai sähköpostitse tietosuojasta vastaavalle tiimille (tiedot alla) tai tietosuojavastaavalle.

11. Sovellettavien lakien edellyttämät tai sallimat tietojen luovutukset

Riippumatta tämän käytännön muista ehdoista, yrityksellä on oikeus luovuttaa tai muulla tavoin käsitellä henkilötietoja koko liiketoimintaa tai sen osaa koskevan minkä tahansa kaupan, sulautumisen, transaktion tai uudelleenjärjestelyjen yhteydessä tai ulkopuolisten auditoijien suorittamia auditointeja varten lakisääteisten vaatimusten täyttämiseksi, tai muissa olosuhteissa, joissa tietojen esittämättä jättäminen heikentäisi yhtiön lakisääteisiä etuja tai sovellettavien lakien näin edellyttäessä tai salliessa. Yritys aikoo toteuttaa asianmukaiset toimenpiteet, kuten tietojen pseudonymisoinnin ja tietojen minimoinnin, suojatakseen henkilötiedot asianmukaisesti tämäntyyppisissä transaktioissa.

Yritys saa myös säännöllisesti luovuttaa henkilötietoja valtion virastoille ja sääntelyviranomaisille (esim. veroviranomaisille), yhteiskunnallisille järjestöille (esim. sosiaaliturvasta vastaavalle hallinnolle), henkilöstöeduista vastaaville tahoille (esim. työterveyshuollon vakuutusyhtiöt), matkustamiseen liittyville kolmansille osapuolille (esim. lennon, hotellihuoneen tai vuokra-auton varaus), tuomioistuimille tai viranomaisten lakisääteisestä pyynnöstä kansallisen turvallisuuden tai muun sovellettavan lakisääteisen velvollisuuden täyttämiseksi, sovellettavien lakien mukaisesti.

Sovellettavien lakien niin edellyttäessä yritys ei luovuta henkilöstön jäsenen henkilötietoja kolmannelle osapuolelle ilman henkilön kirjallista suostumusta.

12. Muiden huollettavien ja sukulaisten henkilötiedot

Jos henkilöstön jäsen luovuttaa yritykselle huollettaviensa, perheenjäsentensä ja/tai sukulaistensa henkilötietoja (esim. tukiasioiden hoitoa ja/tai hätätapauksia varten), henkilöstön jäsenen on ilmoitettava kyseisille henkilöille siitä, että yritys käsittelee heidän henkilötietojaan näissä tarkoituksissa ja tässä käytännössä kuvatulla tavalla ja että heillä on pääsyoikeus omiin henkilötietoihinsa ja oikeus oikaista ja poistaa tiedot sovellettavien lakien mukaisesti sekä tarvittaessa pyydettävä heidän lupansa henkilötietojen käsittelyyn (ja tietojen siirtoon maihin, joissa ei välttämättä noudateta yhtä tiukkaa henkilötietojen suojaustasoa kuin heidän kotimaassaan) tämän käytännön mukaisesti.

13. Henkilöstön jäsenten tiedustelut ja rikkomusepäilyistä ilmoittaminen

Henkilöstön jäsenellä on oikeus tiedustella mitä tahansa sovellettaviin lakeihin liittyvää asiaa tietosuojasta vastaavalta tiimiltä tai paikalliselta tietosuojavastaavalta, mikäli sellainen on nimitetty. Epäilyt tai tiedonsaantipyynnöt voi lähettää myös:

Sähköposti: privacy@venatorcorp.com

EU:ssa toimiville henkilöstön jäsenille: Lisätietoja EU:ssa toimivan henkilöstön valitusprosessista on yrityksen tietosuojakäytännössä, joka löytyy yrityksen intranet-sivustolta.

Asiakirjan versiohistoria

Ohje:	Tietosuoja
Asiakirjan viite:	PRIV-001
Julkaisupäivä:	2018-06-06
Indeksointinumero:	11.1
Arvot:	Lahjomattomuus, Haitattomuus, Tiimityöskentely, Innovaatio, Suorituskyky

Politique mondiale de confidentialité

1. Introduction

Venator Materials PLC, ses filiales et ses sociétés affiliées situées dans le monde entier (ci-après collectivement dénommées « Venator » ou la « Société »), Traitent et Transfèrent des Données à caractère personnel dans la mesure nécessaire ou appropriée à la gestion de votre relation d'emploi ou à toute autre fin explicite et légitime. À cet égard et en conformité avec la présente Politique mondiale de confidentialité (ci-après la « Politique »), la Société s'efforce de respecter les Lois applicables dans la mesure où elles s'appliquent aux salariés et à d'autres personnes.

2. Champ d'application

La présente Politique mondiale de confidentialité informe les salariés sur la manière dont la Société Traite et Transfère les Données à caractère personnel sur le plan local, régional et mondial, y compris, sans s'y limiter les Transferts vers les États-Unis conformément aux Lois applicables. L'équipe Ressources humaines, l'équipe Confidentialité ou, le cas échéant, le Directeur local de la protection des données (ci-après le « DPO ») peuvent fournir davantage d'informations sur les politiques et procédures qui se rapportent aux Données à caractère personnel.

3. Définitions

Lois applicables

Les principes des lois sur la protection des données énoncés dans le Règlement général européen sur la protection des données (ci-après le « RGPD »), les principes des boucliers de protection des données ou les principes de la législation locale sur la protection des données, les plus stricts l'emportant.

Données à caractère personnel

Toute information se rapportant à une personne physique identifiée ou identifiable. Est réputée être une « personne identifiable » une personne physique qui peut être identifiée, directement ou indirectement notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Les catégories de Données à caractère personnel collectées et traitées par la Société ou par un tiers sont identifiées à l'article 5 ci-dessus.

Responsable du traitement

L'entité qui, seule ou de concert avec d'autres, détermine les finalités et les moyens du traitement des Données à caractère personnel.

Sous-traitant

L'entité qui traite des Données à caractère personnel pour le compte du Responsable du traitement.

Traitement

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des Données à caractère personnel, telles que la collecte, l'enregistrement,

l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Transfert

Lorsqu'une partie ou la Société met les Données à caractère personnel à la disposition d'une autre partie ou de la Société par tout moyen.

4. Déclaration sur les boucliers de protection des données

En ce qui concerne les Données à caractère personnel des salariés, la Société reconnaît qu'il existe un régime de protection des données « omnibus » en vertu des Lois applicables. En général, les Lois applicables limitent le Transfert vers les États-Unis des Données à caractère personnel de salariés résidant dans l'UE ou en Suisse, sauf si celles-ci font l'objet d'une « protection adéquate » lors de leur réception aux États-Unis. Afin de gérer cette limitation, la Société a adopté les principes des boucliers de protection des données E-U/UE et E-U/Suisse publiés par l'U.S. Federal Trade Commission à l'égard des Données à caractère personnel que celle-ci reçoit aux États-Unis. La Politique des boucliers de protection des données de la Société, qui se trouve sur la page intranet RGPD de VenNet ou sur le site Web de l'U.S. Federal Trade Commission à https://www.privacyshield.gov/welcome, donne davantage d'informations sur ces boucliers.

5. Définition et collecte des Données à caractère personnel

Les types de Données à caractère personnel que la Société peut recevoir, Traiter et Transférer sur le plan local, régional et mondial, y compris les Transferts vers les États-Unis, ou communiquer à d'autres sociétés Venator ou à des organisations tierces qui lui fournissent des services de gestion ou autres ont été répartis en plusieurs Catégories de Données à caractère personnel. Les Catégories de Données à caractère personnel donnent lieu à des exigences de limitation accrues, en fonction de leur sensibilité, pour les droits d'accès internes et les protections pour la gestion de données physiques exigées des salariés dont les tâches professionnelles légitimes comprennent la gestion des Données à caractère personnel. Les présentes Catégories de Données à caractère personnel ont été conçues pour i) aider les salariés à reconnaître rapidement le degré de sensibilité des Données à caractère personnel en ce qui concerne les droits individuels d'une personne aux fins de protection et de gestion interne et externe et pour ii) améliorer la formation de sensibilisation aux finalités autorisées et limitées de l'accès, de l'utilisation et de la communication pour chaque Catégorie de Données à caractère personnel, afin de les protéger contre le vol, la compromission, la mauvaise utilisation et la consultation par des salariés non autorisés ou d'autres personnes.

Les Catégorie de Données à caractère personnel sont les suivantes :

Catégorie 1 (vert) : Données d'identification professionnelles et coordonnées de la personne

Nom et coordonnées professionnelles de la personne, comme les numéros de téléphone, les adresses professionnelles postale et électronique ;

Catégorie 2 (jaune) : Données à caractère personnel créées par la Société

Informations relatives à l'emploi et au salaire telles que les données sur la rémunération ; les primes et mesures d'incitation ; les informations générales sur les avantages sociaux ; les pensions de retraite ; les performances ; la conformité aux politiques, procédures, normes et lignes directrices en matière d'ESS ainsi qu'aux enquêtes s'y rapportant ; la formation, le développement et la conformité aux politiques, procédures, normes et lignes directrices de la Société ainsi qu'aux enquêtes s'y rapportant ;

Catégorie 3 (orange) : Données à caractère personnel fournies par les personnes

Les informations liées aux données de localisation ou aux identifiants en ligne comme l'adresse du domicile ; les numéros de téléphone du domicile et personnels ; les adresses électronique et IP ; les antécédents professionnels et éducatifs ; les dépenses et les frais de déplacement et l'image ;

Catégorie 4 (rouge) : Données à caractère personnel pouvant être considérées comme sensibles

En fonction des Lois applicables, les Données à caractère personnel pouvant être considérées comme des données sensibles incluent les informations d'identification émises par une autorité administrative ; l'origine raciale ou ethnique, les convictions religieuses ; les informations d'ordre génétique ; les handicaps ou les maladies physiques ou mentales ; l'orientation sexuelle ; les coordonnées personnelles de compte ou de carte bancaires ; l'affiliation à un syndicat ; les antécédents judiciaires et toute sanction reçue pour une offense prouvée ou toute autre Donnée à caractère personnel pouvant nuire gravement à des droits individuels de la personne concernée.

En outre, si un salarié nécessite un visa pour travailler aux États-Unis ou ailleurs, la Société peut demander à celui-ci ainsi qu'à tout membre de sa famille l'accompagnant de lui fournir d'autres Données à caractère personnel ou informations familiales afin de faciliter les demandes de visas. La Société peut également recevoir certaines informations au sujet du conjoint, des membres de la famille ou d'autres personnes à la charge du salarié afin de pouvoir les contacter en cas d'urgence (si celles-ci sont fournies volontairement) et à des fins de gestion d'avantages sociaux.

La Société reçoit des Données à caractère personnel réputées « sensibles » au sens des Lois applicables et dans la mesure permise par celles-ci, par exemple, lorsque cela s'avère nécessaire à l'exécution de la relation d'emploi ou contractuelle. Notamment, la Société peut recevoir et Traiter des Données à caractère personnel sensibles relatives à la santé ou aux handicaps d'un salarié aux fins de la gestion des prestations de santé, des programmes de surveillance médicale, des congés ou de l'adaptation au travail.

Les Données à caractère personnel peuvent être collectées en ligne ou par des formulaires papier avant l'embauche, pendant le processus de recrutement, et aussi pendant la durée d'emploi du salarié.

6. Utilisations des Données à caractère personnel par la Société

La Société peut Traiter et Transférer les Données à caractère personnel liées à un salarié sur le plan local, régional et mondial, y compris aux États-Unis, tel que permis par les Lois applicables, à des fins telles que :

- coordonnées d'urgence
- considération pour un emploi ou une promotion
- gestion du personnel et des tâches
- gestion des performances, de la formation et du développement
- gestion des congés
- facilitation des déplacements et traitement des notes de frais
- gestion de la rémunération, des primes, des pensions, des avantages sociaux et des mesures d'incitation
- gestion des prestations de santé, de l'indemnisation des travailleurs et des programmes de surveillance médicale
- gestion des programmes liés à la rémunération des cadres
- gestion des flux de travail et de la continuité
- budgétisation et planification
- planification de la relève
- vente, fusion ou réorganisation de l'entreprise
- enquêtes personnelles liées à l'entreprise
- traitement des demandes de visas et des permis de travail
- considérations liées à la loi et à la conformité exigeant d'enquêter, de vérifier les comptes et d'appliquer les politiques, procédures, lignes directrices et normes de la Société
- respect des exigences et réglementations sociales, fiscales et légales applicables
- mesures de sécurité informatique en vue de prévenir les intrusions externes ou internes
- accès au réseau et assistance informatique de la Société
- communication liée à l'entreprise
- facilitation de la collaboration sociale sur le réseau de la Société
- préservation ou défense des droits légaux de la Société en réponse à des demandes ou dans le cadre de contentieux lié à l'entreprise
- gestion des doléances et des revendications
- annuaires de coordonnées
- mailing de communications de la Société

La Société peut Traiter et Transférer des Données à caractère personnel telles que des fichiers de journaux ou des adresses IP, dans la mesure permise par les Lois applicables, aux fins de prévention, détection ou investigation d'intrusions externes ou internes dans les systèmes informatiques de celle-ci.

En outre, la Société peut Traiter des Données à caractère personnel dans le cadre de toute enquête de l'équipe Éthique et conformité. Cela inclut les Données à caractère personnel de la personne portant plainte (dans la mesure où cette personne s'est identifiée), les Données à caractère personnel de la personne qui fait l'objet de la plainte et les Données à caractère personnel de toute autre personne qui nous assiste dans les investigations de la Société. La nature des Données à caractère personnel Traitées dépend de la nature du signalement reçu et peut inclure des Données à caractère personnel sensibles. La Société ne conservera ces Données à caractère personnel que le temps qu'elles sont utiles à l'enquête de l'équipe Éthique et conformité ou nécessaires pour des raisons légales.

7. Traitement et transferts de Données à caractère personnel

Afin de Traiter les Données à caractère personnel, la Société peut être obligée de les conserver dans son système informatique Ressources humaines ou dans d'autres plates-formes ou systèmes informatisés ou électroniques et de les Transférer sur le plan local, régional et mondial, y compris les Transferts vers les États-Unis, ou communiquer à d'autres sociétés Venator ou à des organisations tiers qui lui fournissent des services de gestion ou autres, sous réserve de la mise en place de mesures de protection appropriées.

Tel que nécessaire en lien avec les présentes fins, l'équipe Ressources humaines, les superviseurs ou responsables fonctionnels peuvent Traiter et Transférer des Données à caractère personnel dans le cadre des responsabilités de leur poste et de leurs tâches professionnelles légitimes. Si cela est permis par les Lois applicables, certains salariés de la Société peuvent également accéder aux Données à caractère personnel relatives à l'analyse de trafic et de contenu informatiques liés à l'entreprise ainsi qu'à la surveillance et la maintenance des systèmes d'exploitation. La Société prend des mesures appropriées visant à garantir que ce personnel respecte la confidentialité des Données à caractère personnel.

La Société a l'intention de protéger les Données à caractère personnel conformément aux Lois applicables, que les destinataires soient situés dans l'UE, en Suisse ou ailleurs, y compris dans des pays qui peuvent ne pas offrir le même degré de protection des Données à caractère personnel ou qui ne disposent pas de lois nationales procurant le même degré de protection des Données à caractère personnel. Tout Transfert de Données à caractère personnel vers un pays qui ne fournit pas un niveau adéquat de protection des données au sens des Lois applicables sera effectué en fonction i) du consentement des salariés, ii) d'un Contrat de transfert de données, iii) du programme des boucliers de protection des données ou iv) d'autres mesures de protection appropriées, conformément aux Lois applicables ou à la politique de la Société.

8. Notification et choix

La Société a l'intention d'utiliser les Données à caractère personnel aux fins pour lesquelles celles-ci ont été initialement collectées et non de les communiquer à des tiers dans un but incompatible, sauf avec le consentement approprié des intéressés tel que permis par les principes des boucliers de protection des données ou les normes locales en conformité avec les Lois applicables, ou pour le Traitement des Données à caractère personnel par un Sous-traitant externe qui fournit des garanties suffisantes à la Société concernant les mesures techniques et organisationnelles prises en relation avec la protection des Données à caractère personnel.

Les listes des noms et adresses des Sous-traitants tiers et des systèmes internes informatisés ou électroniques utilisés par la Société exigées par les Lois applicables ainsi que toute liste obligatoire des pays auxquels les Données à caractère personnel sont Transférées peuvent être obtenues auprès de l'équipe Confidentialité.

9. Sécurité des données et intégrité des données

La Société a mis en œuvre des mesures de sécurité techniques et organisationnelles appropriées pour protéger les Données à caractère personnel contre la perte, la mauvaise utilisation, l'accès prohibé, la communication ou encore la modification ou la destruction illicites. Les salariés sont également soumis à certaines obligations de confidentialité liées à la gestion et à la protection des Données à caractère personnel et peuvent faire l'objet de sanctions disciplinaires ou de licenciement s'ils manquent à ces obligations.

La Société bénéficie également de procédures visant à garantir, dans la mesure où cela est approprié ou exigé par les Lois applicables, que les Données à caractère personnel sont fiables

pour l'usage prévu, exactes, complètes et tenues à jour et que la personne peut exercer son droit d'accès ou d'effacement de Données à caractère personnel. À cet égard, l'intéressé est encouragé à mettre à jour ses propres Données à caractère personnel lorsque cela est approprié de sorte qu'elles restent exactes, complètes et à jour. La Société conserve les Données à caractère personnel uniquement pendant la durée exigée par la Procédure de conservation des documents de la Société ou tel que permis par les Lois applicables.

10. Accès aux Données à caractère personnel

Les salariés ou autres personnes ont le droit d'accéder à leurs propres Données à caractère personnel et de les consulter conformément à la Procédure mondiale de confidentialité et aux Lois applicables afin de vérifier leur exactitude et leurs utilisations licites, ce qui peut inclure l'investigation des fins du Traitement, les Catégories de données à caractère personnel concernées et les tiers ou catégories de tiers auxquels leurs Données à caractère personnel sont communiquées. Lorsque cela est approprié ou exigé par les Lois applicables, en ce qui concerne les Données à caractère personnel gérées par la Société ou en son nom, un salarié peut mettre à jour ou corriger toute Donnée à caractère personnel inexacte le concernant. Sous réserve des Lois applicables, un salarié peut également demander que ses Données à caractère personnel soient bloquées ou supprimées. Dans certaines circonstances, toutefois, l'accès peut être refusé : en cas de disproportion entre la charge ou les frais de la fourniture d'accès et les risques posés à la vie privée du salarié, en cas de violation des droits d'autrui, en cas de révélation d'informations commerciales confidentielle, de planification de la relève ou de réorganisation ou en cas de compromission d'une question, d'une fonction ou d'un privilège lié à la conformité, la légalité ou la réglementation. La Société peut avoir le droit ou l'obligation légale de continuer à Traiter les Données à caractère personnel d'un salarié après son départ de la Société dans le cadre de la relation d'emploi ou des responsabilités légales de la Société.

Un salarié doit envoyer des demandes d'accès, de modification ou de suppression de ses Données à caractère personnel, par écrit ou par e-mail, à l'équipe Confidentialité, identifiée ci-dessous ou au Directeur de la protection des données.

11. Communications exigées ou permises par les Lois applicables

Indépendamment de toute autre stipulation de la présente Politique, la Société peut communiquer ou autrement Traiter des Données à caractère personnel dans le cadre de toute vente, fusion, transaction ou réorganisation impliquant l'entreprise, en tout ou en partie ; à des fins de vérifications comptables réalisées par des auditeurs externes tel que nécessaire pour répondre à des exigences légales ; dans d'autres circonstances où la non-communication porterait atteinte aux intérêts légitimes de la Société ou encore tel qu'exigé ou permis par les Lois applicables. L'intention de la Société est de mettre en œuvre des mesures appropriées, telles que la pseudonymisation et la minimisation des données, afin de rechercher une protection appropriée des Données à caractère personnel dans ces types de transactions.

La Société peut également communiquer régulièrement des Données à caractère personnel à des organismes administratifs et à des autorités réglementaires (par exemple, des autorités fiscales), à des organismes sociaux (par exemple, la sécurité sociale), à des prestataires d'avantages sociaux de ressources humaines (par exemple, des assureurs maladie), à des tiers liés aux déplacements (par exemple, pour réserver un vol, une chambre d'hôtel ou une voiture de location), à des tribunaux et autres autorités administratives ou dans la mesure où des autorités compétentes le demandent pour répondre à des exigences de sécurité nationale ou exécutoire ou d'autres obligations légales applicables, conformément aux lois applicable.

Si cela est exigé par les Lois Applicables, la Société ne communiquera pas les Données à caractère personnel d'un salarié à un tiers sans avoir obtenu son consentement écrit.

12. Données à caractère personnel concernant les personnes à charge et les personnes apparentées

Si un salarié fournit à la Société des Données à caractère personnel sur ses personnes à charge, des membres de sa famille ou des personnes qui lui sont apparentées (par exemple, à des fins de gestion des avantages sociaux ou des coordonnées d'urgence), il incombe à celui-ci d'informer ces personnes du Traitement de leurs Données à caractère personnel par la Société à ces fins et de la manière décrite dans la présente Politique, de leurs droits d'accès, de rectification et de suppression conformément aux Lois applicables ainsi que d'obtenir leur consentement, le cas échéant, au Traitement (y compris le Transfert vers des pays qui peuvent ne pas fournir le même degré de protection des Données à caractère personnel que leur pays d'origine) de leurs Données à caractère personnel tel que visé dans les présentes.

13. Questions des salariés et signalement des inquiétudes

Un salarié peut demander des éclaircissements concernant tout problème relevant des Lois applicables à l'équipe Confidentialité ou au Directeur local de protection des données, le cas échéant. Les sujets d'inquiétude ou les demandes d'accès peuvent aussi être transmis:

E-mail : privacy@venatorcorp.com

Les salariés situés dans l'UE trouveront des informations supplémentaires sur la procédure de plainte pour les salariés de l'UE dans la Politique de la Société sur les boucliers de protection des données qui figure sur le site intranet de la Société.

Historique des révisions du document

Politique :	Confidentialité
Référence du document :	PRIV-001
Date de publication :	2018-06-06
Numéro d'index :	11.1
Valeurs :	Intégrité, Zero Harm, Travail d'équipe, Innovation, Performances

Politica Globale sulla Privacy

1. Introduzione

Venator Materials PLC e le sue consociate e affiliate situate in tutto il mondo (collettivamente, "Venator" o "Azienda"), Trattano e Trasferiscono i Dati Personali nella misura necessaria o appropriata per la gestione del rapporto di impiego in essere con Lei o per altre finalità specifiche, esplicite e legittime. A tal proposito e conformemente alla presente Politica Globale sulla Privacy ("Politica"), l'Azienda si impegna a rispettare le Leggi Applicabili nella misura in cui tali leggi si applichino ai collaboratori e ad altri soggetti.

2. Ambito

Questa Politica Globale sulla Privacy ("Politica") fornisce ai collaboratori informazioni su come l'Azienda Tratta e Trasferisce i Dati Personali a livello locale, regionale e globale, compresi, a titolo esemplificativo ma non esaustivo, i Trasferimenti verso gli Stati Uniti conformemente alle Leggi Applicabili. Il Team HR, il Team Privacy o, dove applicabile, il Responsabile per la Protezione dei Dati (Data Protection Officer - "DPO") locale possono fornire ulteriori informazioni sulle politiche e procedure dell'Azienda in materia di Dati Personali.

3. Definizioni

Leggi Applicabili

I principi fondamentali della normativa sulla protezione dei dati come indicati nel General Data Protection Regulation ("GDPR") Europeo, i principi di Privacy Shield (Scudo per la Privacy) o le normative locali sulla protezione dei dati, quale di essi sia il più severo.

Dati Personali

Qualsiasi informazione che riguardi una persona fisica identificata o identificabile. Si definisce identificabile una persona che può essere riconosciuta, direttamente o indirettamente, in particolare facendo riferimento a un identificatore come nome, numero di identificazione, dati della località, identificatore on-line o in riferimento a uno o più fattori specifici della sua identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale. Le categorie di Dati Personali raccolti e Trattati dall'Azienda o da terzi sono descritte nella Sezione 5 di seguito.

Controller dei Dati

L'entità che, in modo indipendente o congiuntamente ad altri, stabilisce gli scopi e i mezzi per il Trattamento dei Dati personali.

Responsabile del trattamento dei dati

L'entità che Tratta i Dati Personali per conto del Controller dei Dati.

Trattare/Trattato/Trattamento

Qualsiasi operazione o insieme di operazioni eseguita/e sui Dati Personali, con e senza l'ausilio di mezzi automatici, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o l'alterazione, il recupero, la consultazione, l'uso, la divulgazione

mediante trasmissione, diffusione o altri metodi, l'allineamento o la combinazione, il blocco, la cancellazione o la distruzione degli stessi.

Trasferire/Trasferito/Trasferimento

Atto con cui una parte o l'Azienda rende disponibili i Dati Personali, con qualunque mezzo, a un'altra parte o all'Azienda.

4. Informativa sul Privacy Shield (Scudo per la Privacy)

Rispetto ai Dati Personali dei collaboratori, l'Azienda riconosce che esiste un regolamento “omnibus” sulla protezione dei dati conformemente alle Leggi Applicabili. Generalmente le Leggi Applicabili limitano il Trasferimento dei Dati Personali dei collaboratori di UE e Svizzera verso gli Stati Uniti, a meno che nel Paese ricevente non esista una "protezione adeguata" per tali Dati Personali. Per risolvere tale limitazione, l'Azienda aderisce ai principi sul Privacy Shield per i trasferimenti U.S./UE e U.S./Svizzera pubblicati dalla Federal Trade Commission statunitense rispetto ai Dati Personali che l'Azienda riceve negli Stati Uniti. Ulteriori informazioni sul Privacy Shield sono disponibili nella Politica aziendale sul Privacy Shield, consultabile alla pagina Intranet GDPR su VenNet, o sul sito Web della Federal Trade Commission statunitense all'indirizzo

5. Dati Personali Definiti e Raccolti

I tipi di Dati Personali che l'Azienda può ricevere, Trattare e Trasferire a livello locale, regionale e globale, compresi i Trasferimenti verso gli Stati Uniti, o divulgati ad altre società Venator o a terze parti che forniscono servizi amministrativi o di altro genere all'Azienda, sono stati suddivisi in Categorie dei Dati Personali. In base alla sensibilità dei Dati Personali, le Categorie dei Dati Personali generano maggiori requisiti di limitazione per i privilegi di accesso interno e le protezioni per la gestione dei dati fisici richiesti per i collaboratori i cui incarichi legati ad attività valide comprendono la gestione dei Dati Personali. Queste Categorie dei Dati Personali sono pensate per (i) aiutare i collaboratori a riconoscere rapidamente la sensibilità relativa dei Dati Personali rispetto ai diritti personali di un individuo per la gestione interna ed esterna e ai fini della protezione, e (ii) migliorare la formazione relativa alla sensibilità sugli scopi di accesso, uso e divulgazione ammissibili e limitati per ciascuna Categoria dei Dati Personali, al fine di di proteggerli da furto, compromissione, uso inappropriato e visualizzazione da parte di collaboratori non autorizzati o altre persone.

Le Categorie dei Dati Personali sono le seguenti:

Categoria 1 (Verde) - Dati di contatto e identificazione lavorativi della persona

Il nome e i dati di contatto lavorativi della persona, come numero/i di telefono del lavoro, indirizzo del luogo di lavoro e indirizzo e-mail aziendale;

Categoria 2 (Giallo) - Dati personali creati dall'Azienda

Informazioni relative al lavoro e allo stipendio, come i dati su retribuzione, bonus e incentivi; informazioni generali su benefit, pensioni, prestazioni, conformità con le politiche, le procedure, gli standard e le linee guida EHS e le relative indagini, formazione, sviluppo e conformità con le politiche, le procedure, gli standard e le linee guida dell'Azienda e le relative indagini;

Categoria 3 (Arancione) - Dati personali forniti dalla persona

Informazioni relative alla località o all'identificatore on-line come indirizzo privato, numero di telefono di casa e qualsiasi altro numero di telefono, indirizzo e-mail e IP personale, esperienze lavorative e studi, viaggi e spese di lavoro, immagine;

Categoria 4 (Rosso) - Dati personali che possono essere considerati sensibili

In base alle Leggi Applicabili, i Dati Personali che possono essere considerati sensibili possono comprendere informazioni d'identificazione emesse dal governo, origine razziale o etnica, credo religioso, informazioni genetiche, stato di salute o disabilità fisica o mentale, orientamento sessuale, dati personali bancari o sulle carte di credito, iscrizione a sindacati, precedenti penali e pene ricevute per reati dimostrati o altri Dati Personali che ostacolano seriamente i diritti personali della persona interessata.

Inoltre, se un collaboratore ha necessità di ottenere un visto per lavorare negli Stati Uniti o in altre località, l'Azienda può chiedere al collaboratore, e ai famigliari che lo accompagnano, di fornire all'Azienda ulteriori Dati Personali o informazioni sulla famiglia per agevolare le richieste di visto. L'Azienda può ricevere inoltre alcune informazioni riguardanti il coniuge del collaboratore, i membri della famiglia o altre persone a carico per eventuale contatto in caso di emergenza (se forniti volontariamente) e per scopi amministrativi in riferimento ai benefit.

L'Azienda riceve i Dati Personali "sensibili" ai sensi e nella misura consentita dalle Leggi Applicabili, ad esempio quando è necessario per la gestione del rapporto di assunzione o di collaborazione. In particolare, l'Azienda può ricevere e Trattare i Dati Personali sensibili relativi allo stato di salute e/o di disabilità di un collaboratore per scopi aziendali di gestione dei benefit per la salute, dei programmi di sorveglianza medica, di gestione dei permessi o di accordi relativi agli incarichi lavorativi.

I Dati Personali possono essere raccolti prima dell'inizio del rapporto di assunzione, durante la procedura di ricerca e selezione e per tutto il periodo di collaborazione, con mezzi on-line e/o in formato cartaceo.

6. Usi Aziendali dei Dati Personali

Per quanto consentito dalle Leggi Applicabili, l'Azienda può trattare e Trasferire i Dati Personali dei collaboratori a livello locale, regionale e globale, compresi gli Stati Uniti, per le seguenti finalità:

- Contatti in caso di emergenza
- Analisi per assunzione o promozione
- Gestione del personale e degli incarichi lavorativi
- Gestione delle performance, formazione e sviluppo
- Gestione dei permessi
- Preparazione viaggi ed elaborazione dei report di spesa
- Gestione di retribuzione, bonus, pensione, benefit e programmi di incentivazione
- Gestione dei benefit per la salute, retribuzione dei lavoratori e programmi di sorveglianza medica
- Gestione di programmi esecutivi legati alla retribuzione
- Gestione e continuità del flusso di lavoro
- Bilancio e pianificazione
- Pianificazione delle successioni
- Vendita, fusione o riorganizzazione delle attività
- Sondaggi personali relativi alle attività
- Elaborazione delle richieste di visto e dei permessi di lavoro

- Considerazioni su conformità e aspetti legali che richiedono indagini, verifiche e applicazione di politiche, procedure, linee guida e standard aziendali
- Conformità con i requisiti e le normative sociali, fiscali e di altra natura applicabili
- Misure di Sicurezza IT per prevenire le intrusioni a livello interno e/o esterno
- Accesso alla rete aziendale e supporto IT
- Comunicazioni aziendali
- Favorire la collaborazione sociale sulla rete aziendale
- Preservare o difendere i diritti legali dell'Azienda in seguito a richieste o durante le controversie relative alle attività
- Gestione di rimostranze e/o reclami
- Repertori personali di contatto
- Mailing di comunicazioni aziendali

Per la prevenzione, il rilevamento o l'indagine di intrusioni a livello esterno e/o interno nei sistemi IT dell'Azienda, quest'ultima può Trattare e Trasferire i Dati Personali come file di log o Indirizzi IP nella misura consentita dalle Leggi Applicabili.

L'Azienda, inoltre, può Trattare i Dati Personali in qualsiasi indagine riguardante l'Etica e sulla Conformità. Sono inclusi i Dati Personali riguardanti la persona che presenta il reclamo (nella misura in cui la persona si è identificata), i Dati Personali riguardanti qualsiasi persona che costituisce il soggetto del reclamo e i Dati Personali di qualunque altra persona che fornisce assistenza all'indagine aziendale. La natura dei Dati Personali Trattati dipende dalla natura della segnalazione ricevuta e può comprendere Dati Personali sensibili. L'Azienda conserverà tali Dati Personali per il tempo necessario a svolgere l'indagine sull'Etica e sulla Conformità o a soddisfare motivi legali.

7. Trasferimento e Trattamento dei Dati Personali

Per il Trattamento dei Dati Personali, l'Azienda potrebbe avere necessità di archiviarli nel sistema informativo delle Risorse Umane dell'Azienda o in altri sistemi o piattaforme informativi o elettronici dell'Azienda e di Trasferirli a livello locale, regionale e globale, compresi gli Stati Uniti, o di divulgarli ad altre società Venator o terze parti che forniscono servizi amministrativi o diversi all'Azienda, sempre con le dovute tutele.

Se necessario in relazione a tali finalità, il Team Risorse Umane, i manager funzionali o i supervisori possono Trattare e Trasferire i Dati Personali in relazione alle rispettive responsabilità lavorative e agli incarichi legati ad attività valide. Laddove consentito dalle Leggi Applicabili, i Dati Personali possono essere consultati anche da alcuni collaboratori nell'ambito delle analisi di traffico e contenuti IT relativi alle attività aziendali, nonché nel monitoraggio e nella manutenzione dei sistemi operativi. L'Azienda adotta le opportune misure calcolate per garantire che tale personale mantenga la riservatezza rispetto ai Dati Personali.

L'Azienda intende proteggere i Dati Personali in linea con le Leggi Applicabili indipendentemente dal fatto che i destinatari siano ubicati all'interno dell'Unione Europea o della Svizzera o meno, compresi i Paesi che potrebbero non offrire lo stesso livello di protezione dei Dati Personali o i Paesi che potrebbero non avere leggi nazionali che offrono lo stesso livello di protezione dei Dati Personali. Qualsiasi Trasferimento di Dati Personali verso un Paese che non offre un adeguato livello di protezione dei dati ai sensi delle Leggi Applicabili, sarà eseguito sulla base di (i) il consenso del collaboratore, (ii) un Accordo per il Trasferimento dei Dati, (iii) il Programma Privacy Shield, oppure (iv) altre tutele adeguate conformemente alle Leggi Applicabili o alla politica dell'Azienda.

8. Notifica e Scelta

L'Azienda intende usare i Dati Personali per le finalità per cui tali Dati Personali sono stati originariamente raccolti e non intende divulgare i Dati Personali a terze parti per scopi non coerenti, salvo in caso di specifico consenso delle persone interessate, come indicato dai principi di Privacy Shield o dalle normative locali, conformemente alle Leggi Applicabili, o per il Trattamento dei Dati Personali da parte di un Incaricato esterno che fornisca all'Azienda sufficienti garanzie in merito ai provvedimenti tecnici e organizzativi adottati per la protezione dei Dati Personali.

Il Team Privacy può richiedere e ottenere qualsiasi elenco richiesto dalle Leggi Applicabili dei nomi e indirizzi degli Incaricati terzi e dei sistemi informatici ed elettronici interni utilizzati dall'Azienda, nonché qualsiasi elenco obbligatorio dei Paesi verso cui sono Trasferiti i Dati Personali.

9. Sicurezza e Integrità dei Dati

L'Azienda ha implementato le appropriate misure di sicurezza tecniche e organizzative per proteggere i Dati Personali da perdita, uso improprio, accesso non autorizzato, divulgazione, modifica non autorizzata o distruzione. Anche i collaboratori sono soggetti a determinati obblighi di riservatezza relativi alla gestione e alla protezione dei Dati Personali e possono essere soggetti a sanzioni disciplinari o rescissione del rapporto di collaborazione se non rispettano tali obblighi.

Inoltre l'Azienda mantiene attive le procedure pensate per garantire, nella misura appropriata o richiesta dalle Leggi Applicabili, che i Dati Personali siano affidabili per l'uso previsto nonché precisi, completi e aggiornati, e che la persona possa esercitare il proprio diritto di accedere ai Dati Personali o di cancellarli. A tal proposito, si raccomanda alle persone di aggiornare sempre i propri Dati Personali, se appropriato, per mantenerli precisi, completi e attuali. L'Azienda conserva i Dati Personali solo per il periodo richiesto dalla Procedura Aziendale di Conservazione dei Documenti o per il periodo consentito dalle Leggi Applicabili.

10. Accesso ai Dati Personali

I collaboratori o le altre persone hanno il diritto di accedere e consultare i propri Dati Personali conformemente alla Procedura Globale sulla Privacy e alle Leggi Applicabili per verificarne l'accuratezza e l'uso legittimo, tra cui indagare sulle finalità del Trattamento, sulle categorie dei Dati Personali interessati e sui terzi o categorie di terzi a cui sono divulgati i propri Dati Personali. Laddove appropriato o richiesto dalle Leggi Applicabili, relativamente ai Dati Personali conservati dall'Azienda o per conto dell'Azienda, il collaboratore può aggiornare o correggere i Dati Personali non corretti che lo riguardano. In base alle Leggi Applicabili, il collaboratore può chiedere inoltre che i propri Dati Personali siano bloccati o cancellati. In alcune circostanze, tuttavia, l'accesso può essere negato laddove l'onere o il costo relativi a tale accesso possono essere esagerati rispetto ai rischi per la privacy del collaboratore, i diritti di altri possono essere violati, possono essere rivelate informazioni commerciali riservate o programmi di successione o dati di riorganizzazione, o laddove una questione di conformità, legale o normativa, una funzione o un privilegio possono essere pregiudicati o compromessi. Dopo la fine del rapporto di lavoro, l'Azienda può essere autorizzata, o può essere imposto dalla legge, a continuare il Trattamento dei Dati Personali del collaboratore in relazione al rapporto di lavoro concluso o alle responsabilità legali dell'Azienda.

Il collaboratore deve inviare la richiesta di accesso, modifica o cancellazione dei propri Dati Personali, per iscritto o via e-mail, al Team Privacy identificato di seguito o al Responsabile della Protezione dei Dati.

11. Divulgazioni Richieste o Consentite dalle Leggi Applicabili

Indipendentemente da qualsiasi altra clausola della presente Politica, l'Azienda può divulgare o altresì Trattare i Dati Personali nell'ambito di qualsiasi vendita, fusione, transazione o riorganizzazione che coinvolga le attività, tutte o in parte, o per finalità di verifiche contabili svolte da revisori esterni nella misura necessaria a soddisfare i requisiti normativi, o in altre circostanze che senza l'imposizione della non divulgazione potrebbero pregiudicare i legittimi interessi dell'Azienda, o nella misura richiesta o consentita dalle Leggi Applicabili. L'Azienda intende implementare le misure appropriate, come la pseudonimizzazione e la minimizzazione dei dati, per ottenere la protezione adeguata dei Dati Personali in questi tipi di transazioni.

Inoltre l'Azienda può divulgare regolarmente i Dati Personali ad agenzie governative ed enti normativi (ad es. autorità fiscali), ad organizzazioni sociali (ad es. amministrazione del sistema di previdenza sociale), ai provider di servizi per le risorse umane (ad es. istituti di assicurazione malattia), terze parti relative a viaggi (ad es. prenotazione di voli e camere d'albergo o noleggio auto), tribunali e altre corti e autorità governative o nella misura imposta dalle richieste di legge avanzate da pubbliche autorità per soddisfare i requisiti di sicurezza nazionale o di applicazione o altri obblighi di legge applicabili, conformemente alle Leggi Applicabili.

Laddove richiesto dalle Leggi Applicabili, l'Azienda non divulgherà a terze parti i Dati Personali dei consulenti senza aver ottenuto il loro consenso scritto.

12. Dati Personali relativi a Dipendenti e Persone Collegate

Qualora un collaboratore fornisca all'Azienda i Dati Personali relativi ai propri dipendenti, famigliari e/o persone collegate (ad es. per la gestione dei benefit e/o allo scopo di contatto in caso di emergenza), è responsabilità del collaboratore informare tali persone circa il Trattamento dei loro Dati Personali da parte dell'Azienda per tali finalità e con le modalità descritte nella presente Politica, sui loro diritti di accesso, modifica e cancellazione conformemente alle Leggi Applicabili, nonché ottenere il loro consenso, ove necessario, al Trattamento (compreso il Trasferimento verso Paesi che possono non offrire lo stesso livello di protezione dei Dati Personali rispetto al loro Paese d'origine) dei loro Dati Personali come indicato nella presente Politica.

13. Richieste dei Collaboratori e Segnalazione Problemi

Il collaboratore può chiedere spiegazioni su qualsiasi questione riguardante le Leggi Applicabili al Team Privacy o al Responsabile locale per la Protezione dei Dati, se esiste. Le richieste di chiarimento o accesso possono anche essere inviate:

E-mail: privacy@venatorcorp.com

Per ulteriori informazioni sulla procedura di reclamo per i collaboratori con sede in UE, questi ultimi possono consultare la Politica aziendale di Privacy Shield disponibile sul sito Intranet dell'Azienda.

Storia della Revisione del Documento

Regolamento:	Privacy
Riferimento Documento:	PRIV-001
Data pubblicazione:	2018-06-06
N. indice:	11.1
Valori:	Integrità, Zero Harm, Lavoro in team, Innovazione, Performance

Dasar Privasi Global

1. Pendahuluan

Venator Materials PLC, syarikat subsidiari dan anggota gabungan yang terletak di seluruh dunia (secara kolektif, “Venator” atau “Syarikat”), Memproses dan Memindahkan Data Peribadi, setakat yang diperlukan atau bersesuaian untuk pentadbiran hubungan pekerjaan anda atau mana-mana tujuan lain yang telah dinyatakan, jelas dan sah. Sehubungan dengan itu dan untuk mematuhi Dasar Privasi Global (“Dasar”) ini, Syarikat berusaha untuk mematuhi Undang-undang yang Berkenaan setakat mana yang terpakai kepada rakan sekutu dan kepada individu lain.

2. Skop

Dasar Privasi Global (“Dasar”) ini menyediakan maklumat kepada rakan sekutu tentang cara Syarikat Memproses dan Memindahkan Data Peribadi peringkat tempatan, wilayah dan global, termasuk tetapi tidak terhad kepada Pemindahan ke A.S. mengikut Undang-undang yang Berkenaan. Pasukan HR, Pasukan Privasi, atau, jika berkenaan, Pegawai Perlindungan Data tempatan (“DPO”), boleh menyediakan maklumat lanjut tentang dasar dan prosedur Syarikat yang berkaitan dengan Data Peribadi.

3. Definisi

Undang-undang Yang Berkenaan

Prinsip undang-undang perlindungan data sebagaimana yang ditetapkan dalam Peraturan Perlindungan Data Umum Eropah (“GDPR”), prinsip Perisai Privasi atau undang-undang perlindungan data tempatan, yang mana lebih ketat.

Data Peribadi

Apa-apa maklumat berkaitan dengan orang sebenar yang dikenal pasti atau boleh dikenal pasti. Orang yang boleh dikenal pasti ialah orang yang boleh dikenal pasti secara langsung atau tidak langsung, khususnya dengan merujuk kepada pengecam seperti nama, nombor pengenalan, data lokasi, pengecam dalam talian atau kepada satu atau lebih faktor yang khusus kepada identiti fizikal, fisiologi, genetik, mental, ekonomi, budaya atau sosialnya. Kategori Data Peribadi yang dikumpulkan dan Diproses oleh Syarikat atau pihak ketiga boleh dikenal pasti dalam Seksyen 5 di bawah.

Pengawal Data

Entiti yang secara bersendirian atau bekerjasama dengan orang lain yang menentukan tujuan dan cara Pemprosesan Data Peribadi.

Pemproses Data

Entiti yang Memproses Data Peribadi bagi pihak Pengawal Data.

Proses/Diproses/Memproses

Mana-mana pengendalian atau set pengendalian yang dilaksanakan pada Data Peribadi, sama ada secara automatik atau tidak, seperti pengumpulan, perakaman, penyusunan, penstrukturan, penyimpanan, penyesuaian atau pengubahan, mendapatkan semula, perundingan, penggunaan,

pendedahan melalui penghantaran, penyebaran atau sebaliknya menjadikan tersedia, penjajaran atau penggabungan, pengehadan, pemadaman atau pemusnahan.

Pindah/Dipindahkan/Memindahkan

Apabila satu pihak atau Syarikat menjadikan Data Peribadi tersedia, dengan apa sahaja cara pun, kepada pihak lain atau Syarikat.

4. Pernyataan Perisai Privasi

Berkenaan dengan Data Peribadi rakan sekutu, Syarikat mengakui bahawa terdapat suatu rejim perlindungan data “omnibus” menurut Undang-undang yang Berkenaan. Undang-undang yang Berkenaan secara amnya mengehadkan Pemindahan Data Peribadi rakan sekutu di EU atau Switzerland ke A.S., melainkan jika terdapat “perlindungan yang mencukupi” untuk Data Peribadi tersebut apabila diterima di A.S. Untuk menangani sekatan ini, Syarikat mematuhi prinsip-prinsip Perisai Privasi A.S./EU dan A.S./Swiss yang diterbitkan oleh Suruhanjaya Perdagangan Persekutuan A.S. berhubung dengan Data Peribadi yang diterima oleh Syarikat di A.S. Maklumat lanjut tentang Perisai Privasi boleh didapati di Dasar Perisai Privasi Syarikat, yang terletak di halaman intranet GDPR di VenNet, atau di laman web Suruhanjaya Perdagangan Persekutuan A.S. di https://www.privacyshield.gov/welcome.

5. Data Peribadi yang Ditakrifkan dan Dikumpul

Jenis Data Peribadi yang boleh diterima oleh Syarikat, Diproses dan Dipindahkan di peringkat tempatan, serantau dan global, termasuk Pemindahan ke A.S., atau didedahkan kepada syarikat Venator lain atau organisasi pihak ketiga yang menyediakan pentadbiran atau perkhidmatan lain kepada Syarikat, telah dibahagikan kepada Kategori Data Peribadi. Kategori Data Peribadi mencetuskan peningkatan keperluan sekatan, berdasarkan sensitiviti Data Peribadi, untuk keistimewaan akses dalaman dan perlindungan pengendalian data fizikal yang diperlukan untuk rakan sekutu yang mana tugas berkaitan perniagaan sah termasuk pengendalian Data Peribadi. Kategori Data Peribadi ini direka bentuk untuk (i) membantu rakan sekutu untuk mengenal pasti dengan pantas sensitiviti Data Peribadi tersebut yang berkaitan dengan hak peribadi seseorang individu untuk pengendalian dalaman dan luaran serta untuk tujuan perlindungan dan (ii) meningkatkan latihan kesedaran berkaitan tujuan akses yang dibenarkan dan terhad, penggunaan dan pendedahan bagi setiap Kategori Data Peribadi, untuk melindunginya daripada kecurian, terjejas, penggunaan yang salah dan dilihat oleh rakan sekutu atau individu lain yang tidak dibenarkan.

Kategori Data Peribadi adalah seperti berikut:

Kategori 1 (Hijau) - Kenalan Individu dan Data Pengenalan Perniagaan

Nama individu dan maklumat kenalan yang berkaitan dengan perniagaan seperti nombor telefon tempat kerja, alamat perniagaan dan alamat e-mel;

Kategori 2 (Kuning) - Data Peribadi yang Dibuat oleh Syarikat

Maklumat berkaitan pekerjaan dan gaji seperti data pampasan; bonus dan insentif; maklumat umum tentang faedah; pencen persaraan; prestasi; pematuhan terhadap dasar, prosedur, piawaian dan garis panduan EHS dan penyiasatan berkaitan; latihan dan pembangunan dan pematuhan terhadap dasar, prosedur, piawaian dan garis panduan Syarikat serta penyiasatan berkaitan;

Kategori 3 (Jingga) - Data Peribadi yang Disediakan oleh Individu

Maklumat yang berkaitan dengan data lokasi atau pengecam dalam talian seperti alamat rumah; rumah dan mana-mana nombor telefon peribadi; alamat e-mel dan IP; kerja dan latar belakang pendidikan; perjalanan dan perbelanjaan perniagaan dan imej;

Kategori 4 (Merah) - Data Peribadi Yang Boleh Dianggap Sebagai Sensitif

Bergantung pada Undang-undang yang Berkenaan, Data Peribadi yang boleh dianggap data sensitif, termasuk maklumat pengenalan yang dikeluarkan oleh kerajaan; bangsa atau etnik, kepercayaan agama; maklumat genetik; keadaan kesihatan fizikal atau mental atau kecacatan; orientasi seksual; maklumat perbankan peribadi atau kad pembayaran; keahlian kesatuan sekerja; sejarah jenayah dan apa-apa hukuman yang diterima untuk kesalahan yang terbukti atau apa-apa Data Peribadi lain yang menghalang dengan teruk hak peribadi orang terjejas.

Di samping itu, jika seseorang rakan sekutu perlu mendapatkan visa untuk bekerja di A.S. atau di tempat lain, Syarikat boleh meminta rakan sekutu, dan mana-mana ahli keluarga yang menyertai, untuk menyediakan Data Peribadi tambahan atau maklumat keluarga kepada Syarikat untuk membantu permohonan visa. Syarikat juga mungkin menerima maklumat tertentu tentang pasangan suami isteri, ahli keluarga atau tanggungan lain untuk perhubungan kecemasan (jika secara sukarela disediakan) dan untuk tujuan pentadbiran faedah.

Syarikat menerima Data Peribadi yang “sensitif” dalam ertinya dan setakat yang dibenarkan di bawah Undang-undang yang Berkenaan, seperti apabila perlu untuk pelaksanaan hubungan pekerjaan atau kontrak. Secara khususnya, Syarikat boleh menerima dan Memproses Data Peribadi yang sensitif yang berkaitan dengan kesihatan dan/atau ketidakupayaan rakan sekutu untuk urusan perniagaan iaitu pentadbiran manfaat kesihatan, program pengawasan perubatan, pentadbiran cuti, atau penyesuaian tugasan kerja.

Data Peribadi boleh dikumpulkan sebelum permulaan pekerjaan seperti semasa proses pengambilan dan juga sepanjang tempoh pekerjaan rakan sekutu sama ada melalui kaedah dalam talian dan/atau dalam bentuk kertas.

6. Penggunaan Data Peribadi oleh Syarikat

Syarikat boleh Memproses dan Memindahkan Data Peribadi di peringkat tempatan, di peringkat serantau dan di peringkat global, termasuk di A.S., berkaitan dengan rakan sekutu untuk tujuan, seperti yang dibenarkan oleh Undang-undang yang Berkenaan, seperti yang berikut:

- Perhubungan Kecemasan
- Pertimbangan untuk pekerjaan atau kenaikan pangkat
- Pentadbiran kakitangan dan tugasan kerja
- Pengurusan prestasi, latihan dan pembangunan
- Pentadbiran cuti
- Memudahkan perjalanan dan memproses laporan perbelanjaan
- Pentadbiran pampasan, bonus, pencen, faedah dan program insentif
- Pentadbiran manfaat kesihatan, pampasan pekerja dan program pengawasan perubatan
- Pentadbiran program berkaitan pampasan eksekutif
- Pengurusan dan kesinambungan aliran kerja
- Belanjawan dan perancangan
- Perancangan penggantian
- Penjualan, penggabungan atau penyusunan semula perniagaan
- Kajian peribadi berkaitan dengan perniagaan
- Memproses permohonan visa dan permit kerja

- Pertimbangan pematuhan dan undang-undang yang memerlukan penyiasatan, pengauditan dan penguatkuasaan dasar, prosedur, garis panduan dan piawaian Syarikat
- Pematuhan terhadap keperluan sosial, cukai dan keperluan undang-undang dan peraturan lain yang berkenaan
- Langkah-langkah Keselamatan IT untuk mencegah pencerobohan dalaman dan/atau dalaman
- Akses rangkaian syarikat dan sokongan IT
- Komunikasi berkaitan perniagaan
- Memudahkan kerjasama sosial di rangkaian Syarikat
- Melindungi atau mempertahankan hak undang-undang Syarikat berikutan tuntutan atau semasa litigasi berkaitan perniagaan
- Pentadbiran rungutan dan/atau tuntutan
- Direktori kenalan peribadi
- Perhubungan komunikasi Syarikat melalui mel

Untuk pencegahan, pengesanan atau penyiasatan pencerobohan luaran dan/atau dalaman ke sistem IT Syarikat yang membolehkan Syarikat Memproses dan Memindahkan Data Peribadi seperti fail log atau alamat IP setakat yang dibenarkan oleh Undang-undang yang Berkenaan.

Sebagai tambahan, Syarikat boleh Memproses Data Peribadi sebagai sebahagian daripada penyiasatan Etika & Pematuhan. Ini termasuk Data Peribadi berkenaan si pengadu (sehingga tahap yang mereka dikenal pasti), Data Peribadi tentang sebarang individu yang menjadi subjek aduan dan Data Peribadi individu lain yang membantu kami dengan penyiasatan Syarikat. Sifat Data Peribadi yang Diproses bergantung kepada jenis laporan yang diterima dan mungkin termasuk Data Peribadi yang sensitif. Syarikat hanya akan menyimpan Data Peribadi tersebut selagi ia relevan untuk penyiasatan Etika & Pematuhan atau diperlukan atas alasan undang-undang.

7. Pemindahan dan Pemprosesan Data Peribadi

Untuk Memproses Data Peribadi, mungkin perlu untuk Syarikat menyimpan data dalam sistem maklumat Sumber Manusia Syarikat atau sistem atau platform elektronik atau berkomputer yang lain Syarikat dan Memindahnya di peringkat tempatan, serantau dan global, termasuk ke A.S., atau mendedahkannya kepada syarikat Venator lain atau organisasi pihak ketiga yang menyediakan pentadbiran atau perkhidmatan lain kepada Syarikat, tertakluk kepada perlindungan yang bersesuaian.

Seperti yang perlu berkaitan dengan tujuan ini, Pasukan Sumber Manusia, pengurus atau penyelia fungsian boleh Memproses dan Memindahkan Data Peribadi berkaitan dengan tanggungjawab pekerjaan mereka dan tugas yang berkaitan dengan perniagaan yang sah. Sekiranya dan di mana dibenarkan oleh Undang-undang yang Berkenaan, , Data Peribadi juga boleh diakses oleh rakan sekutu tertentu dalam Syarikat yang berkaitan dengan trafik IT dan analisa kandungan berkaitan perniagaan dan pemantauan serta penyelenggaraan sistem pengoperasian. Syarikat mengambil langkah-langkah yang sewajarnya untuk memastikan bahawa kakitangan tersebut mengekalkan kerahsiaan berkenaan dengan Data Peribadi.

Syarikat berhasrat untuk melindungi Data Peribadi selaras dengan Undang-undang yang Berkenaan tanpa mengira sama ada penerima berada di dalam atau di luar EU atau Switzerland, termasuk di negara-negara yang tidak mungkin menawarkan tahap perlindungan Data Peribadi yang sama atau negara yang tidak mempunyai undang-undang negara yang menyediakan perlindungan Data Peribadi yang sama. Mana-mana Pemindahan Data Peribadi kepada negara yang tidak menyediakan perlindungan data pada tahap yang mencukupi mengikut maksud Undang-undang yang Berkenaan, akan dibuat berdasarkan (i) persetujuan rakan sekutu, (ii)

Perjanjian Pemindahan Data, (iii) Program Perisai Privasi, atau (iv) perlindungan lain yang bersesuaian mengikut Undang-undang yang Berkenaan atau dasar Syarikat.

8. Notis dan Pilihan

Syarikat berhasrat untuk menggunakan Data Peribadi untuk tujuan yang Data Peribadi tersebut dikumpulkan pada asalnya dan tidak berniat untuk mendedahkan Data Peribadi tersebut kepada mana-mana pihak ketiga untuk tujuan yang tidak konsisten, kecuali dengan persetujuan yang sewajarnya daripada individu berkenaan sebagaimana yang dibenarkan di bawah prinsip Perisai Privasi atau piawaian tempatan mengikut Undang-undang yang Berkenaan, atau untuk Pemprosesan Data Peribadi oleh Pemproses luaran yang memberikan jaminan yang mencukupi kepada Syarikat berkaitan dengan langkah-langkah teknikal dan organisasi yang diambil berkaitan dengan perlindungan Data Peribadi.

Mana-mana senarai yang dikehendaki oleh Undang-undang yang Berkenaan tentang nama dan alamat Pemproses pihak ketiga dan sistem berkomputer atau elektronik dalaman yang digunakan oleh Syarikat serta mana-mana senarai yang dikehendaki bagi negara-negara Data Peribadi Dipindahkan yang boleh diperoleh daripada Pasukan Privasi.

9. Keselamatan Data dan Integriti Data

Syarikat telah melaksanakan langkah-langkah keselamatan teknikal dan organisasi yang bersesuaian untuk melindungi Data Peribadi daripada kehilangan, penyalahgunaan, akses tanpa izin, pendedahan atau pengubahan atau pemusnahan tanpa kebenaran. Rakan sekutu juga tertakluk kepada tanggungjawab kerahsiaan tertentu yang berkaitan dengan pengendalian dan perlindungan Data Peribadi dan boleh dikenakan tindakan disiplin atau ditamatkan pekerjaan jika mereka gagal mematuhi tanggungjawab ini.

Syarikat juga mengekalkan prosedur yang direka bentuk untuk membantu memastikan setakat yang bersesuaian atau dikehendaki oleh Undang-undang yang Berkenaan, bahawa Data Peribadi adalah boleh dipercayai untuk kegunaannya yang dirancang dan tepat, lengkap serta terkini dan individu berkenaan boleh menggunakan hak mereka untuk mengakses atau memadam Data Peribadi. Sehubungan ini, individu digalakkan untuk mengemas kini Data Peribadi mereka sendiri dengan sewajarnya untuk memastikan data tersebut tepat, lengkap dan terkini. Syarikat mengekalkan Data Peribadi hanya selagi diperlukan oleh Prosedur Penyimpanan Dokumen Syarikat atau sebagaimana yang dibenarkan oleh Undang-undang yang Berkenaan.

10. Akses kepada Data Peribadi

Rakan sekutu atau individu lain mempunyai hak untuk mengakses dan menyemak Data Peribadi mereka sendiri mengikut Prosedur Privasi Global dan Undang-undang yang Berkenaan untuk mengesahkan ketepatan dan penggunaan data tersebut yang sah, yang termasuk membuat pertanyaan tentang tujuan Pemprosesan, kategori Data Peribadi yang berkenaan, serta pihak ketiga atau kategori pihak ketiga, kepada mereka Data Peribadi didedahkan. Di mana bersesuaian atau dikehendaki oleh Undang-undang yang Berkenaan, berkaitan dengan Data Peribadi yang dikekalkan oleh atau bagi pihak Syarikat, seseorang rakan sekutu boleh mengemas kini atau membetulkan apa-apa Data Peribadi yang tidak tepat tentang diri mereka sendiri. Tertakluk kepada Undang-Undang yang Berkenaan, seseorang rakan sekutu juga boleh meminta Data Peribadi mereka disekat atau dipadamkan. Walau bagaimanapun, dalam sesetengah keadaan, akses boleh dinafikan jika beban atau perbelanjaan menyediakan akses tidak sepadan dengan risiko kepada privasi rakan sekutu berkenaan, di mana hak orang lain akan dilanggar, di mana maklumat komersial sulit atau perancangan penggantian atau maklumat penstrukturan semula akan didedahkan, atau di mana hal berkaitan pematuhan, perundangan atau peraturan, fungsi atau keistimewaan, akan terprejudis atau terjejas. Selepas meninggalkan Syarikat, Syarikat mungkin

berhak atau dikehendaki oleh undang-undang untuk terus memproses Data Peribadi rakan sekutu berkaitan dengan hubungan pekerjaan atau tanggungjawab undang-undang Syarikat.

Rakan sekutu hendaklah menghantar permintaan untuk akses, pindaan atau pemadaman Data Peribadi mereka, secara bertulis atau melalui e-mel, kepada Pasukan Privasi, yang dikenal pasti di bawah atau Pegawai Perlindungan Data.

11. Pendedahan yang Diperlukan atau Dibenarkan Oleh Undang-Undang yang Berkenaan

Tanpa menghiraukan apa-apa peruntukan lain dalam Dasar ini, Syarikat boleh mendedahkan atau sebaliknya memproses Data Peribadi dalam konteks apa-apa penjualan, penggabungan, transaksi atau penyusunan semula yang melibatkan semua atau sebahagian perniagaan, atau untuk tujuan audit yang dijalankan oleh juruaudit luar apabila diperlukan untuk memenuhi keperluan berkanun, atau dalam keadaan lain apabila tanpa pendedahan akan menjejaskan kepentingan sah Syarikat, atau sebagaimana yang diperlukan atau dibenarkan oleh Undang-undang yang Berkenaan. Adalah menjadi niat Syarikat untuk melaksanakan langkah-langkah yang bersesuaian, seperti penyamaran dan pengurangan data, untuk mendapatkan perlindungan Data Peribadi yang bersesuaian dalam urus niaga seperti ini.

Syarikat juga boleh mendedahkan Data Peribadi secara kerap kepada agensi kerajaan dan pengawal selia (cth., pihak berkuasa cukai), pertubuhan sosial (cth., pentadbiran keselamatan sosial), penyedia faedah sumber manusia (cth., insurer kesihatan), pihak ketiga yang berkaitan dengan perjalanan (cth., untuk menempah penerbangan, bilik hotel atau kereta sewa), mahkamah dan pihak berkuasa tribunal dan kerajaan yang lain atau setakat yang dikehendaki oleh permintaan yang sah daripada pihak berkuasa awam untuk memenuhi keperluan keselamatan negara atau penguatkuasaan atau kewajipan undang-undang lain yang terpakai, mengikut Undang-undang yang Berkenaan.

Sekiranya dan apabila diminta oleh Undang-undang yang Berkenaan, Syarikat tidak akan mendedahkan Data Peribadi rakan sekutu kepada mana-mana pihak ketiga tanpa mendapat kebenaran bertulis.

12. Data Peribadi tentang Tanggungan dan Orang Yang Berkaitan

Sekiranya rakan sekutu menyediakan Syarikat dengan Data Peribadi tentang tanggungan, ahli keluarga dan/atau orang yang berkaitan dengan mereka (cth., untuk pentadbiran faedah dan/atau tujuan perhubungan kecemasan), adalah menjadi tanggungjawab rakan sekutu untuk memaklumkan individu berkenaan tentang Pemprosesan Data Peribadi mereka oleh Syarikat untuk tujuan tersebut dan mengikut cara yang diperihalkan dalam Polisi ini, tentang hak akses, pembetulan dan pemadaman mengikut Undang-undang yang Berkenaan, dan termasuk untuk mendapatkan persetujuan mereka, jika perlu, kepada Pemprosesan (termasuk Pindahan ke negara-negara yang mungkin tidak memberikan tahap perlindungan Data Peribadi yang sama seperti di negara asal mereka) Data Peribadi mereka seperti yang ditetapkan dalam Dasar ini.

13. Pertanyaan dan Kebimbangan Pelaporan Rakan Sekutu

Seorang rakan sekutu boleh bertanya tentang apa-apa isu berkaitan Undang-undang yang Berkenaan dengan Pasukan Privasi atau Pegawai Perlindungan Data tempatan, sekiranya ada. Kebimbangan atau permintaan akses juga boleh dihantar kepada:

47198 Duisburg, Germany
E-mel: privacy@venatorcorp.com

Bagi rakan sekutu di EU, maklumat tambahan tentang proses aduan untuk rakan sekutu EU disediakan dalam Dasar Perisai Privasi Syarikat, yang terletak di laman intranet Syarikat.

Sejarah Semakan Dokumen

Dasar:	Privasi
Rujukan Dokumen:	PRIV-001
Tarikh Keluaran:	2018-06-06
Nombor Indeks:	11.1
Nilai:	Integriti, Kemudaratan Sifar, Kerja Berpasukan, Inovasi, Prestasi

全球隐私政策

1. 简介

Venator Materials PLC及其全球子公司和附属公司（统称为“Venator”或“本公司”）处理和传输个人数据，以出于管理您的雇用关系或任何其他指定、明确和合法目的而有必要或适当为限。在这方面且根据本全球隐私政策（“政策”），本公司努力遵守适用于员工和其他个人的适用法律。

2. 范围

本全球隐私政策（“政策”）为员工提供关于本公司如何在本地、区域和全球范围内处理和传输个人数据的信息，包括但不限于，根据适用法律传输到美国。 人力资源团队、隐私团队或当地的数据保护官（“DPO”）可提供关于本公司有关个人数据的政策和程序的更多信息。

3. 定义

适用法律

《欧洲通用数据保护条例》（“GDPR”）、隐私保护原则或本地数据保护立法规定的数据保护法律原则，以较严格者为准。

个人数据

任何与已识别或可识别的自然人有关的信息。 可识别的人士是指可直接或间接通过参考姓名、身份号码、位置数据、在线识别符等标识符或特定于其身体、生理、遗传、精神、经济、文化或社会身份的一个或多个因素识别身份的人士。 本公司或第三方收集和处理的个人数据类别列于下文第 5 节。

数据监控员

单独或与他人共同确定处理个人数据的目的和手段的实体。

数据处理员

代表数据监控员处理个人数据的实体。

处理/已处理/正在处理

对个人数据进行的任何操作或一组操作，无论是否采用自动方式，如收集、记录、组织、构建、存储、改编或更改、检索、咨询、使用、传播披露、散播或以其他方式提供、对齐或组合、限制、清除或破坏。

传输/已传输/正在传输

一方或本公司以任何方式向另一方或本公司提供个人数据的情况。

4. 隐私保护声明

就员工的个人数据而言，本公司确认，存在符合适用法律的“综合”数据保护制度。 适用法律通常限制欧盟或瑞士员工的个人数据传输到美国，除非在美国收到此类个人数据时有“适当保护”。为应对此限制，本公司坚持美国联邦贸易委员会公布的美国/欧盟和美国/瑞士隐私保护原则，该原则涉及本公司在美国收到的个人数据。有关隐私保护的更多信息可在本公司的隐私保护政策中找到，该政策位于VenNet的GDPR内联网页面上，或位于美国联邦贸易委员会网站上：https://www.privacyshield.gov/welcome。

5. 定义和收集的个人数据

本公司在本地、区域和全球范围内接收、处理和传输（包括传输到美国，或向其他Venator公司或向本公司提供管理或其他服务的第三方组织披露）的个人数据类型已被划分为个人数据类别。
个人数据类别触发了基于个人数据敏感度的增强限制要求，用于内部访问权限和物理数据处理保护，其有效业务相关任务包括处理个人数据的员工需要达到该要求。这些个人数据类别旨在：(i)
协助员工迅速认识到此类个人数据对于出于个人内部和外部处理和保护目的的个人权利的相对敏感性，及 (ii)
加强对每种个人数据类别的访问、使用和披露的许可和有限目的的认识培训，以避免被盗、泄露、不当使用和未经授权的员工或其他个人查看。

个人数据类别如下：

类别1（绿色） – 个人的联系方式和业务识别数据

个人姓名和业务相关的联系信息，例如，工作电话号码、企业地址和电子邮件地址；

类别2（黄色） – 本公司创建的个人数据

与工作和薪资有关的信息，如薪酬数据；奖金和奖励；关于福利的一般信息；退休金；绩效；EHS政策、程序、标准和准则的遵守情况及相关调查；培训和制定及遵守本公司政策、程序、标准和准则以及相关调查；

类别 3（橙色） – 个人提供的个人数据

与位置数据或在线标识符有关的信息，例如，家庭住址；家庭和任何个人电话号码；电子邮件和 IP 地址；工作和教育背景；商务旅行和费用；及肖像；

类别 4（红色） – 被视为敏感的个人数据

根据适用法律，被视为敏感数据的个人数据（包括政府颁发的身份信息）；种族或民族血统、宗教信仰；遗传信息；身体或心理健康状况或残疾；性取向；个人银行或支付卡信息；工会会员资格；犯罪历史和因已证实的罪行而受到的任何惩罚或任何其他严重妨碍受影响个人的个人权利的个人数据。

此外，如果员工需要获得在美国或其他地方工作的签证，本公司会要求员工及其随行家属向本公司提供额外的个人数据或家庭信息，以协助签证申请。本公司还会收到关于员工的配偶、家庭成员或其他家属的紧急联系方式（如果自愿提供的话）以及用于福利管理目的的某些信息。

在适用法律允许的范围内，本公司需要收到适用法律所指的“敏感”个人数据，例如，履行雇用关系或合同关系时。 特别是，本公司会收到并处理与员工的健康和/或残疾相关的敏感个人数据，以用于管理健康福利、医疗监督计划、假期管理或工作职责住宿的业务目的。

可在雇用开始之前（例如在招聘过程中）收集个人数据，也可以通过在线方式和/或纸质形式在员工的整个受雇过程中收集。

6. 本公司对于个人数据的使用

在适用法律许可的范围内，本公司可在本地、区域和全球范围内（包括在美国）处理和传输与员工有关的个人数据，其目的如下：

- 紧急联系
- 考虑就业或晋升
- 管理人员和工作职责
- 绩效管理和培训与发展
- 假期管理
- 便利差旅和处理费用报告
- 管理薪酬、奖金、退休金、福利和激励计划
- 管理健康福利、工人薪酬和医疗监督计划
- 管理高管薪酬相关计划
- 工作流程管理和连续性
- 预算和计划
- 接任计划
- 业务的出售、合并或重组
- 业务相关的个人调查
- 处理签证申请和工作许可
- 需要调查、审计和执行本公司政策、程序、准则和标准的合规性和法律考虑
- 遵守适用的社会、税务和其他法律要求和规定
- 可防止外部和/或内部入侵的 IT 安全措施
- 本公司网络访问和 IT 支持
- 业务相关的沟通
- 促进本公司网络的社会协作
- 在追索后或在业务相关的诉讼中维护或捍卫本公司的合法权利
- 管理申诉和/或索赔
- 个人联系人目录
- 邮寄本公司通信

为了预防、检测或调查本公司 IT 系统的外部和/或内部入侵，本公司会在适用法律允许的范围内处理和传输个人数据，例如日志文件或 IP 地址。

另外，本公司可能会在开展任何道德与合规调查时处理个人数据。这包括有关投诉之人的个人数据（自身能够发现的程度）、有关投诉对象的个人数据以及帮助我们完成公司调查之人的个人数据。所处理个人数据的性质取决于收到报告的性质，可能会包含敏感的个人数据。本公司将仅保留与道德及合规调查相关的个人数据以及法律所要求的必要个人数据。

7. 个人数据传输和处理

为了处理个人数据，本公司需要将其存储在本公司的人力资源信息系统或本公司的其他计算机化或电子系统或平台中，并将其传输到本地、区域和全球（包括美国），或向其他 Venator 公司或为本公司提供管理或其他服务的第三方组织披露，并采取适当的保护措施。

出于这些目的的需要，人力资源团队、职能经理或主管可以处理和传输与其工作职责和有效业务相关任务有关的个人数据。如果并且在适用法律允许的情况下，本公司某些与业务相关的IT流量和内容分析以及操作系统监控和维护有关的员工也会访问个人数据。 本公司采取适当措施确保此类人员对个人数据保密。

本公司打算根据适用法律保护个人数据，无论收件人位于欧盟或瑞士境内还是境外，包括未提供相同个人数据保护水平的国家或没有规定相同级别个人数据保护之国家法律的国家。 基于下述各项向未提供适用法律所指适当数据保护水平的国家传输个人数据：(i) 员工同意书；(ii) 数据传输协议；(iii) 隐私保护计划；或 (iv) 符合适用法律或本公司政策的其他适当保障措施。

8. 通知和选择

本公司打算将个人数据用于最初收集此类个人数据的目的，并且不打算向任何第三方披露个人数据用于其他目的，除非受影响的个人根据适用法律并在隐私保护原则或当地标准允许的范围内给出适当的同意，或由外部处理员处理个人数据，但该处理员须向本公司提供与保护个人数据有关的技术和组织措施的充分担保。

可向隐私团队获取适用法律规定的本公司使用的第三方处理员和内部计算机化或电子系统名称和地址清单，以及向其传输个人数据的规定国家清单。

9. 数据安全和数据完整性

本公司已实施适当的技术和组织安全措施，以避免个人数据丢失、滥用、未经授权访问、披露或未经授权更改或破坏。 员工还受到与处理和保护个人数据相关的某些保密义务的规限，如果他们未能履行这些义务，则会受到纪律处分或解雇。

本公司还维持相关程序，旨在确保在适用法律适当或规定的范围内，对于其预期用途而言，个人数据可靠且准确、完整和最新，并且个人可行使其访问或清除个人数据的权利。 在这方面，鼓励个人在适当时更新其个人数据，以保持其准确性、完整性和最新。 本公司仅在本公司的文件保留程序或适用法律允许的范围内保留个人数据。

10. 访问个人数据

员工或其他个人有权根据全球隐私程序和适用法律访问和查看其个人数据，以验证其准确性和合法使用情况，包括查询处理目的、涉及的个人数据类别以及向其披露个人数据的第三方或第三方类别。 在适用法律适当或规定的范围内，关于由本公司或本公司代表维护的个人数据，员工可更新或更正关于其自身的任何不准确的个人数据。 根据适用法律，员工也可以要求阻止或删除其个人

数据。然而，在某些情况下，如果提供访问的负担或费用与员工的隐私风险不相称、他人的权利受到侵犯、将会披露机密商业信息或接任计划或重组信息或者合规、法律或监管事宜、职能或特权受到损害或危害，则不可进行访问。 离开本公司后，本公司有权或依法就雇用关系或本公司的法律责任继续处理员工个人数据。

员工应通过书面形式或通过电子邮件向下面指定的隐私团队或数据保护官发送访问、修改或删除请求。

11. 适用法律要求或允许的披露

无论本政策是否有任何其他规定，在涉及全部或部分业务的出售、合并、交易或重组，或涉及外部审计师进行审计而有必要满足法定要求，或者在其他情况下，不披露信息会损害本公司的合法利益，或者适用法律规定或允许的情况，本公司可披露或以其他方式处理个人数据。本公司有意采取适当措施，例如假名化和最少数据收集，力图适当保护这些交易类型中的个人数据。

本公司还会根据适用法律，定期向政府机构和监管机构（如税务机关）、社会组织（如社会保障管理机构）、人力资源福利提供商（如健康保险公司）、与旅行有关的第三方（例如预订航班、旅馆房间或租车）、法院和其他法庭及政府当局或根据公共事业机构的法律要求规定披露个人数据，以满足国家安全或执法要求或其他适用法律义务。

如果适用法律要求，本公司不得在未获得其书面同意的情况下向任何第三方披露员工的个人数据。

12. 有关家属和相关人员的个人数据

如果员工向本公司提供关于其家属、家庭成员和/或相关人员的个人数据（例如出于福利管理和/或紧急联系目的），则该员工有责任以本政策所述的方式通知上述人员本公司为了上述目的而处理其个人数据、其可根据适用法律访问、更正和删除的权利，以及在必要时征得其同意后，根据本政策处理其个人数据（包括传输到并未提供与本国相同水平的个人数据保护的国家）。

13. 员工查询和报告疑虑

员工可向隐私团队或当地数据保护官询问有关适用法律的任何问题。 疑虑或访问请求也可直接发给

电子邮件：privacy@venatorcorp.com

对于欧盟的员工，本公司的隐私保护政策提供有关欧盟员工投诉流程的更多信息，该政策位于本公司的内部网站上。

文档修订历史

政策：	隐私
文件参考号：	PRIV-001
发布日期：	2018 年 6 月 6 日
索引号：	11.1
价值观：	正直、零伤害、团队合作、创新、绩效