Table of Contents

1.0 Purpose

This Employee Data Policy ("Employee Data Policy") explains what types of Personal Information or PI, including Personally Identifiable Information or PII, Constellis Holdings, LLC and its subsidiaries and affiliates (collectively the "Company" or "Constellis") may collect about its employees, job applicants, and candidates (collectively "Individuals") and how Personal Information may be used.

2.0 Policy Summary

Constellis is a global company with its headquarters in the United States. To facilitate Constellis' global operations, Constellis may transfer and access Personal Information from around the world, including from other countries in which it has operations. A list of Constellis' global offices is available https://constellis.com/who-we-are/global-footprint for reference. This means that Personal Information may be used, processed, and transferred to the United States and other countries or territories and those countries or territories may not offer the same level of data protection as the country where you reside,

including the European Economic Area. In some cases, Individuals may provide Personal Information to third parties with which Constellis works. This could be, for example, a third-party website where an Individual can apply for a job at Constellis, or take advantage of services made available to its employees. The use of such third-party websites may be governed by separate terms of use and privacy policies promulgated by those third parties.

3.0 Scope

This Policy applies to all Company business units. While this Employee Data Policy is intended to describe the broadest range of the Company's information processing activities globally, those processing activities may be more limited in some jurisdictions based on the restrictions of their laws. For example, the laws of a particular country may limit the types of personal information the Company can collect or the manner in which it processes that information. In those instances, the Company will adjust its internal policies and practices to reflect the requirements of local law.

4.0 Definitions

4.1 Personal Information

Personal Information or PI, including Personally Identifiable Information or PII, for purposes of this Employee Data Policy means any information that (1) directly identifies an individual *OR* (2) indirectly identifies an individual, such as when used in combination with other information. Personal information does not include such information if it is anonymous or if it has been rendered de-identified by removing personal identifiers. Examples of Personal Information include:

- Name, social security number or other taxpayer/government identification number
- Gender
- Marital status
- An individual's photograph
- Employee ID number
- Home address
- Home phone number
- Personal email address
- Names of family members
- Date of birth

4.2 Sensitive Personal Information.

Sensitive Personal Information is a subset of personal information that may be more sensitive in nature for the individual concerned. Examples of Sensitive Personal Information include:

- Race and ethnic information
- Sexual orientation
- Political/religious beliefs
- Social security or other taxpayer/government issued identification numbers
- Financial information
- Health or medical information
- Criminal records
- And in some regions, such as the European Union, trade union membership

4.3 Employment-related Information

In addition to the above, the Company also collects employment-related information, which is a subset up Personal Information. Examples of employment-related information include:

- Employee identification number and emergency contacts
- Residency and work permit status, military status, nationality, and passport information
- Payroll information and banking details
- Wage and benefit information
- Retirement account information
- Sick pay, Paid Time Off ("PTO"), retirement accounts, pensions, insurance, and other benefits information (including the gender, age, nationality, and passport information for any spouse, minor children, or other eligible dependents and beneficiaries)
- Information from interviews and phone-screenings
- Date of hire, date(s) of promotions(s), work history, technical skills, educational background, professional certifications and registrations, language capabilities, and training records
- Employee stock information
- Beneficiary and emergency contact information
- Forms and information relating to the application for or changes to, employee health and welfare benefits; including, short and long term disability, medical, and dental care
- Height, weight, and clothing sizes, likeness in photographs and/or videos, physical limitations and special needs
- Records of work absences, vacation/paid time off entitlement and requests, salary history and expectations, performance appraisals, letters of appreciation and commendation, and disciplinary and grievance procedures
- Where permitted by law and applicable, the Company may collect the results of credit and criminal background checks, the results of drug and alcohol testing, screening, health certifications, driver's license number, vehicle registration, and driving history
- Information required for the Company to comply with laws, the requests and directions of law enforcement authorities or court orders (e.g., child support and debt payment information)
- Acknowledgements regarding Company policies, including employee handbooks, ethics and/or conflicts of interest policies, and computer and other corporate resource usage policies
- Information captured on security systems, including Closed Circuit Television ("CCTV") and key card entry systems
- Voicemails, e-mails, correspondence, documents, and other work product and communications created, stored, or transmitted using Company networks, applications, devices, computers, or communications equipment
- Date of resignation or termination, reason for resignation or termination, information relating to administering termination of employment (e.g., references)
- Letters of offer and acceptance of employment
- Resumes or CV's, cover letters, previous and/or relevant work experience or other experience, education, transcripts, or other information provided to the Company in support of an application and/or the application and recruitment process
- References and interview notes
- Information relating to any previous applications made to Constellis and/or any previous employment history with Constellis

5.0 Policy

5.1 What Personal Information Is Collected

The Company collects and maintains different types of Personal Information and Sensitive Personal Information listed in Section 4.0 about Individuals in accordance with applicable law and only when necessary to effectuate the employer-employee relationship as described in Section 5.3.

5.2 How Data Is Collected

Generally, the Company collects Personal Information directly from Individuals in circumstances where they provide Personal Information (e.g., by submitting job applications, during interviews, the onboarding process, signing up for direct deposit, or enrolling in benefits or services). However, in some instances, the Personal Information collected has been inferred to an Individual based on other information provided, through interactions with the Company, or from third parties. Generally, the Company collects Personal Information from third parties either because the Individual gave the Company express permission to do so, the permission was implied by the Individual's actions, or because the Individual provided explicit or implicit permission to the third party to provide the Personal Information to the Company.

Where permitted or required by applicable law or regulatory requirements, the Company may collect Personal Information about Individuals without their knowledge or consent. The Company reserves the right to monitor the use of its premises, equipment, devices, computers, network, applications, software, and similar assets and resources. In the event such monitoring occurs, it may result in the collection of Personal Information. This monitoring may include the use of CCTV cameras in and around Company premises.

5.3 Use of Collected Personal Information

The Company uses Personal Information for its lawful business purposes. These uses include:

- To manage all aspects of an employee's employment relationship, including, but not limited to, the establishment, maintenance, and termination of employment relationships. Examples of activities related to this include: determining eligibility for initial employment, including the verification of references and qualifications; pay and benefit administration; the issuance and management of stock options and restricted stock units; corporate travel and other reimbursable expenses; development and training; absence monitoring; project management; auditing, compliance, and risk management activities; conflict of interest reporting; employee communications; performance evaluation; disciplinary actions; grievance and internal investigation activities; career management, including the assessment of qualifications for a particular job or task; processing employee work-related claims (e.g., worker's compensation, insurance claims); succession planning; relocation assistance; obtaining and maintaining insurance; employee engagement programs, to include surveys; the provision of employee-related services; and other general operations, administrative, financial, and human resources-related purposes.
- Assisting employees with obtaining an immigration visa or work permit, where required
- For use in video conferencing
- For the maintenance of personnel directories
- For administering occupational safety and health programs
- To protect the safety and security of its workforce, guests, property, and assets (including controlling and facilitating access to and monitoring activity on and in Company premises, and

activity using Company computers, devices, networks, communications, and other assets and resources)
- To investigate and respond to claims against the Company
- To maintain emergency contact and beneficiary details
- To comply with applicable laws (e.g., health and safety, employment laws, office of foreign asset controls regulations, tax laws), including judicial or administrative orders regarding individual employees (e.g., garnishments, child support payments)
- To carry out any additional purposes that the Company advises employees of (and if applicable law requires express consent for such additional use or disclosure the Company will request it and employees will be free to agree or decline)
- Carry out other purposes as part of Company business activities when reasonably required

5.4 Sharing Personal Information

Employee Personal Information may be shared, including to Company affiliates, subsidiaries, and other third parties, as follows:

- Where an Individual requests that Personal Information be shared or has provided consent
- When using or collaborating with third parties in the operation of Company business, including in connection with providing many of the benefits and services offered employees (e.g., human resources information systems, financial investment service providers, wellness program service providers, and insurance providers). When the Company shares Personal Information with third parties and/or service providers, it requires that the third party and/or service provider limit its use or disclosure of Personal Information only to the extent necessary to provide the requested services to the Company and in a manner consistent with the use and disclosure provisions of this Employee Data Policy and applicable law.
- The Company may buy or sell businesses and other assets. In such transactions, Personal Information is generally one of the transferred business assets and the Company reserve the right to include as an asset in any such transfer. Also, in the event that the Company, or substantially all of its assets, are acquired, Personal Information may be one of the transferred assets.
- Where required by law, by order or requirement of a court, administrative agency, or government tribunal, which includes in response to a lawful request by public authorities, including to meet national security or law enforcement requirements or in response to legal process
- If the Company determines it is necessary or desirable to comply with the law or to protect or defend its rights or property
- As necessary to protect the rights, privacy, safety, or property of an identifiable person or group; or to detect, prevent, or otherwise address fraud, security or technical issues; or to protect against harm to the rights, property, or safety of Constellis, its users, applicants, candidates, employees, or the public; or as otherwise required by law
- Where the Personal Information is public
- To seek advice from Company lawyers, accountants, consultants, auditors, and other professional advisers

5.5 Access to and Updating of Collected Personal Information

When required by applicable law, Individuals can ask to see the Personal Information that the Company holds about them. If an Individual wants to review, verify, or correct their Personal Information, please submit a request to the Company point of contact to whom the Personal Information was disclosed,

or in the alternative to legal@constellis.com. When requesting access to Personal Information, please note that the Company may request specific information from the Individual to enable the Company to confirm the Individual's identity and right to access, as well as to search for and provide Personal Information that the Company holds. An Individual's right to access the Personal Information that the Company holds about them is not absolute. There are instances where applicable law or regulatory requirements allow or require the Company to refuse to provide some or all of the Personal Information that the Company has collected. In addition, the Personal Information may have been destroyed, erased or made anonymous. In the event that the Company cannot provide an Individual with access to their Personal Information and if required by law, the Company will inform the Individual of the reasons why, subject to any legal or regulatory restrictions.

If during a review, the Company determines that Personal Information is inaccurate or incomplete, it will use reasonable efforts to revise it and, if required by law, use reasonable efforts to inform agents, service providers, and/or other third parties, which were provided with inaccurate information, so records in their possession may be corrected or updated.

5.6 Retention of Collected Personal Information

Except as otherwise permitted or required by applicable law or regulatory requirements, the Company will retain Personal Information only for as long as necessary to fulfill the purposes for which the Personal Information was collected (including, for the purpose of meeting any legal, accounting, or other reporting requirements or obligations). Individuals may request that the Company delete the Personal Information collected about him or her. There are instances where applicable law or regulatory requirements allow or require the Company to refuse to delete this Personal Information. In the event that the Company cannot delete an Individual's Personal Information, and if required by law, it will undertake reasonable efforts to inform Individual of the reasons why.

5.7 Requests to Correct or Delete Personal Information or Withdraw Consent

Requests to correct or delete Personal Information or withdraw consent for its collection can be submitted to legal@constellis.com. Any request to correct or delete Personal Information will be reviewed, and subject to the provisions of this Employee Data Policy, the Company's Privacy Policy, and all applicable laws and regulations, processed using reasonable efforts. Importantly, requests may not result in deletion of any information submitted to a third-party provider. If an Individual requires the third-party to delete any Personal Information, they must contact the third party directly to request such deletion.

Notwithstanding that an Individual may have provided their express consent for the Company to use Personal Information for a specific use, that consent may be withdrawn as provided by applicable law. Requests to withdraw previously given consent should be sent to Company point of contact to whom consent was given, or in the alternative to legal@constellis.com.

5.8 Resolving Concerns

Individuals who have questions or concerns regarding the handling of their Personal Information should contact the Company's legal department at legal@constellis.com. Alternatively, Individuals may report concerns or complaints, including information about potential data breaches involving personal information to the CyberSecurity team at itsec@constellis.com or report violations of this Employee Data Policy or law using Constellis' third-party Ethics Hotline, constellis.ethicspoint.com.

5.9 Changes to Employee Data Policy

This Employee Data Policy is reviewed periodically to ensure it accurately captures all types of data collected or any additional or different processing of such data. The Company may, therefore, change this Employee Data Policy at any time. The effective date of each version of this Employee Data Policy is identified below.

5.10 Security of Collected Personal Information

The Company is committed to protecting the security of the Personal Information collected, and it takes reasonable physical, electronic, and administrative safeguards that comply with industry-standard best-practice to help protect the Personal Information from unauthorized or inappropriate access or use.

Related Documents

- **Constellis Privacy Policy**

VERSION HISTORY

Version	Version Date	Author	Description
1.0	12/1/2019	R. Bill	Initial Version