

## **Moog Inc.**

### Notice of Data Privacy for Employees

Revision 7.0

8 Nov 2016

#### **1.0 Introduction/Notice**

Moog Inc., and its subsidiaries (collectively, "Moog"), are required to collect and maintain information about its employees in order to comply with a myriad of governmental and contractual obligations, including providing for the payment of taxes, employee benefits, wages, etc. However, Moog also recognizes the importance of protecting your privacy, and therefore complies with the U.S.-EU Privacy Shield Framework, including the Privacy Shield Principles (the "Principles"<sup>1</sup>). Moog certifies on an annual basis that it adheres to the Privacy Shield Principles of notice, choice, onward transfer, security, data integrity, access, plain language, free and independent recourse and enforcement. To learn more about the Privacy Shield program, and to view Moog's certification, please visit <http://www.privacyshield.gov>. This Notice of Data Privacy Policy for Employees ("Policy") describes the data collected by Moog from its employees and how Moog uses that data. The Federal Trade Commission has enforcement authority over Moog's compliance with the Framework.

Note: Moog remains committed to the U.S.-Swiss Safe Harbor Framework.

Note: It is incumbent on the Operating Groups and Business Units to identify, track and document additional local and/or regional regulations and ensure compliance.

#### **2.0 Collection of Employee Data**

In connection with your employment, Moog may ask you to provide certain information only for limited and specified purposes, including, but not limited to, your name, mailing address, telephone numbers, citizenship, country of residence, country of origin, gender, birth date, marital status, name of dependents, birth date of dependents, occupation of dependents and national identification number. Additionally we may maintain information relating to your employment with the Company including, but not limited to, your employee identification number, business unit/division of employment, department, physical work location, job code, compensation rate, supervisor, work shift, hire and termination date, appraisal dates and ratings, training, skills, educational background, language proficiency, certifications and licenses.

#### **3.0 Use of Employee Data**

The Employee Data collected by Moog will be used for various administrative and record keeping purposes by Moog.

#### **4.0 Disclosure of Employee Data and Accountability for Onward Transfer for Limited and Specified Purposes**

Employee Data will be disclosed to those Moog employees whose job necessitates that they maintain, compile, or otherwise have access to Employee Data. These employees are specifically

---

<sup>1</sup> The European Commission prohibits the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection. In order to provide a streamlined means for U.S. organizations to comply, the U.S. Department of Commerce in consultation with the European Commission developed a "Privacy Shield" framework. The Privacy Shield framework - approved by the EU in July 2016 - allows U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European data protection authorities under European data privacy laws. Certifying to the Privacy Shield assures that EU organizations know that our company provides "adequate" privacy protection, as defined by the Directive.

authorized by Moog and have specific Employee Data responsibilities. Moog may also disclose Employee Data to a third party when it believes, in good faith, that such disclosure is reasonably necessary to comply with any law or to protect the rights, property or safety of another person. Additionally, Moog may disclose Employee Data to a third party employee benefit provider, including but not limited to, employee benefit providers and payroll services. If Moog does disclose data to third party, Moog will ensure that the third party either subscribes to the Principles or Moog will enter into a written agreement with such third party which requires the third party to provide at least the same level of privacy protection as is required by the relevant Principles. The third party agreement will require oversight to ensure compliance and require notice if the third party can/will no longer comply. Upon notice Moog shall stop transfer and remediate. Moog is liable in cases of onward transfer of data to third parties. Lastly, Moog may transfer or otherwise disclose Employee Data in connection with the sale of its business to a third party and retain historical Employee Data only as long as required by law.

## **5.0 Transfer of Employee Data**

Employee Data will be transferred, transmitted and accessed electronically by a limited number of Moog employees (as discussed above) at various Moog locations around the world. Moog has taken, and will continue to take, appropriate technical and organizational measures to protect all Employee Data from destruction, loss, alteration, or unauthorized disclosure or access. Further data as to how Employee Data is transferred, transmitted and accessed electronically and how Moog protects such Employee Data can be found in *Practice for Protection and Transmission of Employee Data* as well as the Moog Policy Statements referred to therein.

## **6.0 Employee Consent**

Unless you withdraw your consent, in writing, you agree to and accept the proposed use, disclosure and transmission of your Employee Data by Moog as set forth in this Policy. Upon any modification of this Policy, Moog will prominently post a revised Policy within five (5) business days of its adoption and provide employees with an opportunity to withdraw his or her consent to any new use or disclosure of his or her Employee Data. If any employee objects to Moog's collection, use, disclosure or transmission of certain Employee Data, Moog will make reasonable efforts to address the concerns of the employee. In no case will an employee be subject to sanction or retaliation for objecting to the collection, use, disclosure or transmission of Employee Data. Any employee who withholds Employee Data or prohibits its collection, use, disclosure or transmission, however, may be disadvantaged as a result of not making the data available. For example, unwillingness to provide data required to use a service or receive a benefit may make an employee ineligible for that service or benefit.

## **7.0 Your Rights Regarding Your Employee Data**

Although your Employee Data is the physical property of Moog, the data contained in the record belongs to you. Upon request in a reasonable notice period, each employee has the right to:

- Obtain a copy of Moog's Policy upon request.
- Inspect his or her Employee Data and be able to correct data where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated. All requests to inspect, correct data must be submitted in writing to the local Human Resources Manager and Privacy Compliance Officer.
- Review Moog's process and procedures for electronically transmitting Employee Data, as set forth in *Practice for Protection and Transmission of Employee Data* as well as the Moog Policy Statements referred to therein.
- Withdraw his or her consent to the continued or future use and disclosure of his or her Employee Data, except as to that Employee Data that Moog determines to be necessary for continued employment.

## **8.0 Moog's Responsibilities Regarding Protecting Employee Data**

Moog is required to:

- Inform employees of Moog's Policy regarding the collection, maintenance, use and disclosure of Employee Data.
- Ensure that Moog's published Policy is current, accurate, comprehensive, prominently displayed, completely implemented, accessible, and conforms to established data privacy principles.
- Abide by the terms of this Policy. In the event that Moog modifies the terms of this Policy, Moog will prominently post a revised Policy which describes all intended uses and disclosures of Employee Data, within five (5) business days of its adoption, and provide employees with an opportunity to withdraw his or her consent to any new use or disclosure of his or her Employee Data.
- Notify the employee if the Company is unable to agree to the employee's requested restriction on the use or disclosure of his or her Employee Data.
- Maintain the privacy of your Employee Data by taking reasonable precautions to protect the data from loss, misuse, unauthorized access, disclosure, alteration and destruction.
- Comply with all laws regarding the privacy of Employee Data including the right to disclose personal information in response to a lawful request by public authorities including to meet national security or law enforcement requirements.
- Ensure commitments as long as data is held.
- Ensure procedures are in place for verifying compliance with its procedures using self-verification procedures and tools.

## **9.0 Complaints**

If you believe Moog has breached its Policy by permitting an unauthorized use, disclosure or transmission of your Employee Data, you may contact or file a complaint with your supervisor. If you are not satisfied with the response or action taken by your supervisor, all such complaints and concerns may then be directed to Moog's Privacy Compliance Officer, Cheryl M. Gray, 400 Jamison Rd., East Aurora, NY 14052 (716) 805-2373. You will not be penalized for filing a complaint. Moog must respond to the complaint within 45 days.

## **10.0 Independent Recourse Mechanism and Access to Free Dispute Resolution**

Moog has chosen the EU Data Protection Authorities (EU DPAs) through The United States Council for International Business (USCIB), acting as a trusted third party on behalf of the European Union (EU) Data Protection Authorities, to serve as an independent recourse mechanism (IRM) for dispute resolution arising from collection, use, and retention of personal information transferred from EU member countries to Moog.

This resource mechanism is available free of charge. The U.S. Department of Commerce agrees to cooperate with the EU Data Protection Authority (DPA) to receive, review and undertake best efforts to facilitate resolution of the of the complaint and respond to the DPA within 90 days.

Moog also commits to binding arbitration at the request of the individual to address any complaint that has not been resolved by other recourse or enforcement mechanism.