Global Privacy Policy

I. Purpose

The purpose of this Policy is to establish the fundamental roles, responsibilities, and policies necessary to implement the privacy principles of the General Motors Company (GM). This Policy is based on GM's Privacy Principles of Notice, Choice and Consent, Collection, Access, Security, Enforcement, and Data Quality, which are consistent with globally recognized fair information privacy principles.

As part of their global operations, GM and its Controlled Subsidiaries, as defined below, Process information about individuals, in particular, information relating to their customers and employees. This information may include Personal Information such as: (1) any information that can be used to distinguish or trace an individual's identity; or (2) any other information that is linked or reasonably linkable to an individual. GM and its Controlled Subsidiaries may acquire Personal Information through numerous channels, such as from vehicles, websites, mobile Apps, dealers, marketing partners, service providers, or via employment procedures. This Policy requires GM and its Controlled Subsidiaries to Process Personal Information in accordance with applicable laws and regulations of its global markets.

II. Executive in Charge, Policy Contact, Policy Interpretations and Policy Deviations

The Executive in Charge of this Policy is the Chief Privacy Officer (CPO). The Contact for this Policy is the Global Privacy Office (GPO). The CPO, with approval from the General Counsel, has been designated as the owner of this Policy, having the authority to approve any revisions thereof. Proposed deviations from the provisions of this Policy must be submitted in writing with justification to the CPO.

III. Applicability

This Policy applies to:

- GM and its Controlled Subsidiaries.
- All employees of GM or its Controlled Subsidiaries including GM employees that are seconded to GM's non-controlled partners or joint ventures.

As to companies and employees of companies in which GM owns 50% or less of the equity, and does not exercise management control, a case-by-case determination, with the support of the GPO, is made by the General Counsel as to whether this Policy applies.

IV. Definitions

"Controlled Subsidiary" is defined as all subsidiaries in which GM owns more than 50% of the equity interest, directly or indirectly, or in which GM exercises management control.

"CPO" is defined as Chief Privacy Officer.

"GPO" is defined as Global Privacy Office.

"Personal Information" may be defined differently in various jurisdictions. Generally, Personal Information includes (1) any information that can be used to distinguish or trace an individual's identity; or (2) any other information that is linked or linkable to an individual. GM and its Controlled Subsidiaries may collect and retain Personal Information in various forms, including electronically and on paper. If Personal Information is altered so that it can no longer reasonably link to an individual, the information is no longer Personal Information. Employees who Process Personal Information must be aware that data protection laws and regulations may restrict or prohibit the use, sharing or cross-border transfer of that information. Please contact the GPO to receive specific information about what constitutes Personal Information in your jurisdiction. Generally, Personal Information may include, but is not limited to, the following:

- Last name plus first initial or first name
- Home address or other physical address, including street name and name of city or town
- E-mail address or other online contact information
- Telephone number
- Social security number or other government-issued personal identifier such as a tax identification number or driver's license number
- Vehicle Identification Number, Vehicle Registration Number, or License Plate Number
- Internet Protocol address
- A persistent identifier (e.g., unique customer number in a cookie)
- Financial account information (account number, credit or debit card numbers or banking information)
- Date of birth with other potentially identifying information, other than last name plus first initial or first name
- Mother's full maiden name with other potentially identifying information
- Medical information (including health, health insurance information, or electronic Protected Health information (ePHI) as otherwise defined by regulations)
- Digitized or electronic signature
- Any other information that is combined with any of the above

"Process" is defined as the collection, use, protection, transfer, storage, alteration, disclosure, sharing, or disposal of Personal Information.

"Sensitive Personal Information" is a subset of "Personal Information" that is generally subject to stricter protections. The definition of "Sensitive Personal Information" varies across jurisdictions. It may include an individual's last name plus first name or initial in combination with one of the following:

- A social security number or other government-issued identifier such as a tax identification number, driver's license number, state-issued ID, or passport number
- Financial account information (account number, credit or debit card numbers or banking information)

- Date of birth (month, day, and year)
- Medical information (including health, health insurance information, or electronic Protected Health information (ePHI) as otherwise defined by regulations)
- An identifier as otherwise defined in the local jurisdiction (e.g., mother's maiden name)

In some jurisdictions, Sensitive Personal Information may include information capable of revealing an individual's race, ethnicity, political opinions, religious beliefs, membership in a trade union, health condition, sexual orientation, or criminal history. Sensitive Personal Information may also include precise location information, biometric information, and genetic information.

V. Policy

GM and its Controlled Subsidiaries must:

- **Comply** with all laws and regulations applicable to our business operations and the Processing of Personal Information.
- **Collect** Personal Information to support legitimate business purposes only.
- Provide reasonable **notice** regarding Processing. As appropriate to the context of collection, notices should inform individuals of the types of Personal Information collected, how the Personal Information will be used, the types of third parties that may receive the Personal Information, whether the Personal Information may be transferred to other countries, the rights individuals may have regarding the Personal Information, and contact information submitting questions or inquiries regarding Processing. An example of this appropriate notice is OnStar's U.S. Consumer Privacy Statement at http://www.onstar.com/privacy
- Provide individuals with reasonable **choice** and obtain **consent** regarding Processing as appropriate to the context of collection, the type of data collected, and the purposes for which it will be used.
- **Process** Personal Information fairly and lawfully as reasonable to support legitimate business purposes and consistent with the context of collection. For example, if a privacy statement notifies a consumer that Personal Information is collected to support a specific service only, but is silent about using that information for marketing purposes, then that information should not be used for marketing purposes absent additional notice or consent as appropriate, or unless such use would be expected in context.
- Take reasonable steps to ensure that the Personal Information collected is **accurate, relevant, up to date, complete**, and consistent with the context of collection.
- Provide individuals with reasonable means, as appropriate, to **review** their Personal Information and to **request correction** of factual inaccuracies in accordance with and subject to applicable laws, GM procedures, and appropriate verification of the individuals' identities.
- **Secure** Personal Information by reasonable and appropriate information protection safeguards to protect against loss and unauthorized access, use, and disclosure.
- **Limit access** to Personal Information to those individuals who have a reasonable need for access in support of legitimate business purposes.

- **Retain** Personal Information only as reasonable to support legitimate business purposes and consistent with the context of collection, or as required by law or GM policy (including GM's Information Lifecycle Management (ILM) Policy).
- **Dispose** of Personal Information in a manner appropriate to the confidential nature of the data and in accordance with GM's ILM Policy.
- Assess whether Processing involves **international transfers** of Personal Information and whether appropriate mechanisms are in place to support those transfers.
- Assess whether Processing involves **disclosing Personal Information to third parties** and implement appropriate safeguards to protect such information following disclosure.
- **Integrate** GM's Privacy Principles into business activities, including, as necessary, agreements and arrangements with third parties, controlled and non-controlled entities and individuals with whom we have a business relationship.
- **Implement** and **maintain procedures** to coordinate enterprise-wide privacy compliance activities, recognizing that certain aspects of compliance should be implemented at the local level. Appropriate procedures should include regular training on privacy and security issues and regular audits or assessments of privacy and security practices.
- **Report** and **respond** to incidents involving potential or actual compromises of Personal Information, as required by law and GM's policies and procedures including reporting potential Personal Information losses using the Global Reporting and Investigations Tool or "GRIT" and following the Personal Information Security Incident or "PISI" process.

Responsibilities

GM Audit Services is responsible for auditing conformity of global business operations with this Policy and for recommending corrective actions, as appropriate.

GM Employees and Employees of Controlled Subsidiaries are responsible for reading, understanding, and complying with this Policy and other related GM policies and directives. This responsibility includes, but is not limited to, protecting Personal Information in their care from improper use and disclosure. GM Employees and Employees of Controlled Subsidiaries who are unsure of their responsibilities shall seek guidance from their Legal Staff representative or the Global Privacy Office. Failure to comply with this Policy may result in disciplinary action up to and including termination, depending on the nature and severity of the violation, and in accordance with applicable law. GM Employees and Employees of Controlled Subsidiaries who suspect violations of this Policy or of any privacy law should report such suspected violations in accordance with established reporting procedures, including the GM Awareline. Those who report suspected violations in good faith will not be subject to retaliation or suffer any adverse action as set forth in GM's Speak Up! Non-Retaliation Policy.

GM's Global Ethics and Compliance Center is responsible to assist in enforcement of this Policy.

GM's Global Privacy Office is responsible for establishing and oversight of this Policy, providing guidance to GM business operations in the implementation of this Policy, developing the strategy and direction for GM's global privacy program, and assisting in the reporting and investigation of potential Personal Information losses through the PISI process. In addition, the GPO will review and comment on proposed privacy legislation, regulations, or other policies that may significantly impact GM business operations,

and will cooperate with government agencies to facilitate timely, reasonable, and business-practical solutions for privacy issues that may arise.

GM Management in charge of GM business units or functions has primary responsibility for compliance and enforcement of this Policy within their respective areas of responsibility. This includes providing guidance for the implementation of this Policy within their respective organizations and, in consultation and coordination with the GPO or GM Legal Staff, implementing processes to monitor compliance with privacy laws applicable to their areas and jurisdictions of operation.