International Data Protection Policy

Revised April 2013

Table of Contents

Statement of Visteon Corporation President and CEO

Visteon Corporation is committed to complying with applicable laws wherever we do business. This is vital to our continued success in an increasingly regulated global marketplace, and also reflects our commitment to conduct business in accordance with the highest legal and ethical standards.

As a U.S.-based company with operations worldwide, including within the European Union, Visteon is subject to regulations under the laws of the United States, the Member States of the European Union, and other countries covering the information we process concerning our employees, customers, suppliers and others.

This International Data Protection Policy, prepared by the Corporate Transactions and Legal Affairs Department and our Office of Data Protection, is intended to help you understand these regulations. Our Data Protection officers and their staff are available to answer any questions you may have. Although the specific technical requirements of the law are beyond the scope of this policy, these requirements establish uniform standards of conduct for employees of Visteon and its subsidiaries worldwide who handle information covered by these regulations.

At Visteon, we require full compliance to this policy to help ensure adherence to applicable data privacy and security laws.

Thank you for your attention to this important matter.

Timothy D. Leuliette
President and CEO
Visteon Corporation

Visteon International Data Protection Policy

1.0 Purpose

This Policy defines requirements to ensure compliance with laws and regulations applicable to Visteon's collection, use, and transmission of Personal Data throughout the world.

2.0 Scope

Visteon is committed to complying with the applicable data privacy and security requirements in the countries in which it and its subsidiaries (the "Company") operate. Because of differences among these jurisdictions, the Company has adopted a data protection Policy which creates a common core of values, policies and procedures intended to achieve nearly universal compliance, supplemented with alternative or additional policies or implementation procedures applicable in those jurisdictions with unique requirements.

This Policy applies to all Visteon full and part time employees, agency employees, employees of Visteon majority-owned subsidiaries, joint venture employees, and all suppliers and vendors who receive Personal Data from Visteon, have access to Personal Data collected or processed by Visteon, or who provide information to Visteon, regardless of geographic location.

3.0 Requirements

3.1 Office of Data Protection

Visteon's compliance program will be overseen by individuals with significant authority and independence. To underscore our commitment to the authority and independence of our compliance oversight efforts and to facilitate the effectiveness of those efforts, the Company has established an Office of Data Protection.

3.1.1 The Office of Data Protection shall be coordinated by the Visteon Chief Compliance Officer.

3.1.2 The individuals identified in Exhibit A have been selected to perform the duties of the Office of Data Protection. The duties of these Data Protection Officers are set forth in this Policy and implementing procedures the Office of Data Protection may adopt, as well as any duties required by applicable law to be performed by a designated Data Protection Officer, including at least the following:

3.1.2.1 Determining whether notification to one or more data protection authorities is required as a result of the Company's current or intended data processing activities.

3.1.2.2 Making any required notifications and keeping such notifications current.

3.1.2.3 Designing an implementing programs for training employees in data protection rules and procedures.

3.1.2.4 Establishing procedures and standard contractual provisions for obtaining compliance with this Policy by vendors, suppliers, and third parties who receive Personal Data from Visteon, have access to Personal Data collected or processed by Visteon, or who provide information to Visteon, regardless of geographic location.

3.1.2.5 Establishing mechanisms for periodic audits of compliance with this Policy, implementing procedures, and applicable law.

3.1.2.6 Establishing, maintaining, and operating a system for prompt and appropriate responses to Data Subject requests to exercise their rights.

3.1.2.7 Ensuring that Visteon's compliance program is kept current.

3.1.2.8 Informing senior managers, officers, and directors of the Company of the potential corporate and personal civil and criminal penalties which may be assessed against the Company and/or its employees for violation of applicable data protection laws.

3.2 Data Protection Principles

The Company has adopted the following principles to govern its use, collection, and transmittal of Personal Data, except as specifically provided by this Policy or as required by applicable laws:

3.2.1 Personal Data shall only be processed fairly and lawfully.

3.2.2 Personal Data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes.

3.2.3 Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or processed.

3.2.4 Personal Data shall be accurate, complete and current as appropriate to the purposes for which they are collected and/or processed.

3.2.5 Personal Data shall not be kept in a form which permits identification of the Data Subject for longer than necessary for the permitted purposes.

3.2.6 Personal Data shall not be collected or processed unless:

3.2.6.1 the Data Subject has provided a valid, informed consent, See Section 3.3;

3.2.6.2 processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;

3.2.6.3 processing is necessary for compliance with a Visteon legal obligation;

3.2.6.4 processing is necessary in order to protect the vital interests of the Data Subject;

3.2.6.5 processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller or in a third party to whom the data are disclosed; or

3.2.6.6 processing is necessary for legitimate interests of Visteon or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the fundamental rights and freedoms of the Data Subject.

3.2.7 Personal Data shall be collected and processed in accordance with the rights of the Data Subjects. See Section 3.8.

3.2.8 Appropriate physical, technical, and procedural measures shall be taken to: (i) prevent and/or to identify unauthorized or unlawful collection, processing, transmittal of Personal Data; and (ii) prevent accidental loss or destruction of, or damage to, Personal Data. See Section 7.0.

3.3 Consents

3.3.1 The Office of Data Protection, in cooperation with the business units, the Corporate Transactions and Legal Affairs Department, and the Chief Information Officer, shall establish systems for the collection and documentation of Data Subject consents to the collection, processing, and/or transfer of Personal Data.

3.3.2 To be valid, consent must be informed, express, and freely given.

3.3.3 If consent is obtained with other written declarations, the request for consent must be made conspicuous.

3.3.4 Consent with regard to Sensitive Data must refer expressly to those data.

3.3.4.1 Consent must be revocable.

3.3.4.2 The consent system shall include provisions for determining what disclosures should or must be made in order to obtain a valid consent, documentation of the date, method and content of the disclosures made, as well as the validity, scope, and volition of the consents given.

3.4 Transfers to Third Parties

3.4.1 Personal Data shall not be transferred to another entity, country or territory, unless reasonable and appropriate steps have been taken to maintain the required level of data protection.

3.4.2 Personal Data may be communicated to third persons only for reasons consistent with the purposes for which the data were originally collected or other purposes authorized by law.

3.4.3 All Sensitive Data transferred outside of the Company or across public communications networks shall be de-identified or shall be protected against unauthorized access by use of encryption.

3.4.4 All transfers of Personal Data to third persons for further processing shall be subject to written agreements. The Office of Data Protection shall, in cooperation with the Corporate Transactions and Legal Affairs Department, develop standard terms and conditions which can be used for this purpose.

3.4.5 EU Personal Data shall not be transferred to a country or territory outside the European Economic Area unless the transfer is made to a country or territory recognized by the EU as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data, or is made in compliance with one of the mechanisms recognized by the EU as providing adequate protection when transfers are made to countries or territories lacking an adequate level of legal protection.

3.4.6 The Company complies with the U.S.- EU Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use and retention of personal information from European Union member countries. The Company has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view the Company's certification, please visit http://www.export.gov/safeharbor/.

3.4.6.1 Notwithstanding the provisions of Subsections 3.4.4 and 3.4.5, Personal Data may be transferred where any of the following apply:

(a) The Data Subject has given consent to the proposed transfer;

(b) The transfer is necessary for the performance of a contract between the Data Subject and the Company, or the implementation of precontractual measures taken in response to the Data Subject's request;

(c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Company and a Third Party;

(d) The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defense of legal claims;

(e) The transfer is required by law;

(f) The transfer is necessary in order to protect the vital interests of the Data Subject; or

(g) The transfer is made from a register which according to laws or regulations is intended to

provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.

3.5 Prevention of New or Expanded Non-Complying Activities

3.5.1 No new or expanded collection or processing activities involving Sensitive Data may be undertaken without first obtaining approval from the Office of Data Protection.

3.5.2 To obtain approval, the business unit shall provide the Office of Data Protection with the information identified in a data processing assessment form and such other information as the Office of Data Protection may request.

3.5.3 The Company's Information Technology Department, in cooperation with the Office of Data Protection, shall establish a procedure for assessing the impact of any new technology uses on the privacy and security of Personal Data. The Information Technology Department shall include such an assessment for each such proposed new or expanded use of technology resources in its application design review process and shall provide such assessments to the Office of Data Protection.

3.5.4 Personnel at all levels of the Company will apply the following guidelines when designing new systems, uses or processes involving Personal Data and/or reviewing or expanding existing activities involving the collection or processing of Personal Data:

3.5.4.1 Collection and use of Personal Data will be avoided or limited when reasonably possible.

3.5.4.2 Personal Data will be de-identified when the purposes of data collection or processing can be at reasonable cost achieved without maintaining personal identification.

3.5.4.3 The purpose(s) of the collecting or processing of Personal Data will be expressly identified by the business unit preparing any new or expanded data collection and processing activity or function.

3.5.4.4 Personal Data may only be used for the purposes for which they were originally collected, plus historical, statistical, scientific, or legally mandated purposes, unless the Data Subject has given consent or an exception set forth in Section 3.2.6 applies.

3.6 Disclosures at the Time of Data Collection

3.6.1 Appropriate disclosures will be made at the time a Data Subject is asked to give consent to the collection or processing of Personal Data, and whenever Personal Data are collected.

3.6.2 Specific information must be disclosed to the Data Subject and/or any other person from whom Personal Data are obtained at the time of collection, unless the Data Subject already has the information. The business unit collecting the information, in cooperation with the Office of Data Protection, must establish technical or administrative means for documenting the fact that the Data Subject already has the information and how.

3.6.3 The foregoing disclosure requirements shall not apply where such disclosure could not be implemented in a reasonable manner with cost and effort proportionate to the importance of the proposed processing, or where applicable law provides an exemption to requirements for disclosure and/or consent.

3.6.4 If no exemption applies, the following information must be disclosed to the Data Subject and/or any other person from whom Personal Data are obtained at the time of collection:

3.6.4.1 The name and address of the Data Controller and, if one has been appointed, the name and address of the Data Controller's EU Member State in-country representative for data privacy.

3.6.4.2 The purpose(s) of collecting, processing, and transmitting the data.

3.6.4.3 Whether the source of the data is under an obligation to supply the data and the consequences of failing to do so.

3.6.4.4 The identities, or at least the categories, of natural or legal persons who will or may receive the data.

3.6.4.5 Whether any transfers of data outside of the European Economic Area may occur and, if so, whether such transfers may be made to a country which has not been determined by the EU to have adequate data protection laws.

3.6.4.6 The terms of the transfer, such as whether it is done pursuant to a procedure approved by a Works Council, a contract embodying the EU Commission's Model Contractual Clauses, The U.S. Safe Harbor procedures, or some other mechanism.

3.6.4.7 The Data Subject's right to access, receive a copy of, erase, and correct the data and the means of exercising those rights.

3.6.4.8 How long Visteon expects or intends the Personal Data to be retained.

3.6.4.9 The procedures available for resolving any disputes about processing of the Data Subject's Personal Data.

3.6.4.10 Any other information necessary to guarantee "fair processing." For example, where the data are to be used in a manner not apparent to the Data Subject, such use should be disclosed.

3.6.5 These disclosures should be given as soon as possible, and preferably at the first point of contact with the Data Subject. In the case of employees, the disclosures should be made in the employment contract (if any). Appropriate disclosures should also be made in any job application form or employee handbook. The disclosures should be made in a manner calculated to draw attention to them.

3.6.6 The disclosures may be given orally, electronically via the Company's intranet or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Office of Data Protection. The receipt or form should be retained along with a contemporaneous record establishing the fact, date, content, and method of disclosure.

3.6.7 If inadequate disclosures are made initially, additional disclosures may have to be made at a later time, and the fact, date, content, and method of these additional disclosures shall be recorded.

3.7 Sources of Personal Data

3.7.1 Personal Data shall be collected only from the Data Subject unless the nature of the business purpose necessitates collection of the data from other persons or bodies, collection from the Data Subject would necessitate disproportionate effort, or collection must be accomplished under emergency circumstances in order to protect an interest of the Data Subject or to prevent serious loss or injury to another person.

3.7.2 If Personal Data are collected from someone other than the Data Subject, the Data Subject must be informed of the following items unless the Data Subject has received the required information by other means, notification would require disproportionate effort, or the law expressly provides for collection, processing or transfer of the Personal Data:

3.7.2.1 The fact of the collection, processing or transfer of the data by the Data Controller;

3.7.2.2 The nature and purposes of the processing;

3.7.2.3 The recipients or categories of recipients of the data;

3.7.2.4 The origin of the data; and

3.7.2.5 The information set forth in section 3.6.4 above.

3.7.3 The business unit, in cooperation with the Office of Data Protection, will create a form or system to document and automate this process as fully as possible.

3.7.4 Notification to a Data Subject should occur promptly, but in no event later than three months from the first collection or recording of the Personal Data by the Company.

3.8 Data Subject Rights

3.8.1 The Office of Data Protection shall establish a system to enable and facilitate exercise of Data Subject rights of access, blockage, erasure, opposition, rectification, and, where appropriate or required by applicable law, a system for giving notice of inappropriate exposure of Personal Data.

3.8.2 Data Subjects shall be entitled to obtain the following information about their own Personal Data upon a request made in compliance with reasonable policies and procedures established, and set forth in writing, by the Office of Data Protection:

3.8.2.1 Whether the Company has stored Personal Data concerning the Data Subject.

3.8.2.2 Whether any of the data are Sensitive Data.

3.8.2.3 The source(s) of the data, if known.

3.8.2.4 The recipients or categories of recipients to whom the data have been or may be transmitted.

3.8.2.5 The purposes of the collection, processing, use and storage of the data.

3.8.2.6 A hard copy of the data in an intelligible form.

3.8.3 The Company shall provide its response to a request under Section 3.8.2 within 40 days of the date the Company receives a written request from the Data Subject and appropriate verification that the requestor is the Data Subject or an authorized legal representative.

3.8.4 Data Subjects shall have the right to require the Company to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

3.8.5 Requests for access to or rectification of Personal Data shall be directed, at the Data Subject's option, to the manager of the business unit responsible for the Personal Data or to the Office of Data Protection.

3.8.6 All business units receiving a Data Subject request for access to Personal Data shall notify the Office of Data Protection.

3.8.7 The Office of Data Protection shall establish a system for logging each request under this Section as it is received and noting the response date.

3.8.8 If the Company cannot respond fully to the request within the time indicated, then the responsible business unit or the Office of Data Protection shall nevertheless provide the following information within the specified time:

- An acknowledgement of receipt of the request.
- Disclosure of responsive information located to date.
- Identification of any requested information or modifications which the Company will not provide, the reason(s) for the refusal, and the procedures for appealing the decision within the Company, if any.
- An estimate of a date by which the remaining responses will be made.
- A statement or estimate of any costs to be paid by the Data Subject.
- The name and contact information of the individual who the Data Subject should contact for follow up.

3.8.9 Where providing the information about the requesting Data Subject would disclose Personal Data about *another* individual, the business unit handling the request must review the data and redact or withhold the information as may be necessary or appropriate to protect *that* person's rights.

3.8.10 The Company will not charge employees for providing the information identified above. The Office of Data Protection may establish reasonable fees to cover the cost of responding to requests from non-employee Data Subjects.

3.8.11 The Office of Data Protection may establish procedures to screen and deny abusively burdensome or repetitive requests by or on behalf of a Data Subject.

3.9 Automated Decision Making

If a business unit engages in any decision making based solely on the automated application of predetermined rules, this must be disclosed to the Data Subjects. The Data Subject must be given the opportunity to (i) review the logic used by the automated system, (ii) supplement the automated system with additional data, and (iii) obtain review of the automated decision by an individual.

3.10 Sensitive Data

3.10.1 Sensitive Data should not be processed unless:

3.10.1.1 Such processing is specifically authorized or required by law.

3.10.1.2 The Data Subject expressly consents.

3.10.1.3 The processing is required for preventive medicine, medical diagnosis, or health care treatment; provided the data are processed by a health professional subject to national law or rules with an obligation of professional secrecy or by another person with an equivalent obligation of secrecy. If the Company is relying upon this medical exemption, all contracts with employees and independent contractors who will have access to the

Sensitive Data must contain confidentiality requirements equivalent to those imposed on health professionals.

3.10.1.4 Where the Data Subject is physically or legally incapable of giving consent, but the processing is necessary to protect a vital interest of the Data Subject. This exemption may apply, for example, where emergency medical care is needed.

3.10.1.5 Data relating to criminal offenses may be processed only by or under the control of an official authority.

3.10.2 If the Company is relying upon one of the exemptions to authorize processing of Sensitive Data, the exemption relied upon, and the basis for the exemptions should be recorded with the data.

3.11 Direct Marketing

When Personal Data are transferred for direct marketing, the Data Subject should be able to “opt-out” from having his/her data used for such purposes at any stage.

3.12 Data Quality Assurance

3.12.1 Each business unit shall take steps to assure that Personal Data it collects or processes is complete and accurate in the first instance. Data must be accurate and updated in such a way as to give a true picture of the current situation of the Data Subject.

3.12.2 The Company shall correct data which it knows to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification. Inaccurate data must be erased and replaced by corrected or supplemented data.

3.12.3 Personal Data must be kept only for the period necessary for permitted uses. When defining a permitted use for data, the business unit shall establish a sunset or review date for the stated purpose.

3.12.4 Personal Data should be erased if their storage violates any of the data protection rules or if knowledge of the data are no longer required by the Company or for the benefit of the Data Subject. See Record Retention Policies.

3.12.5 Personal Data should be blocked, rather than erased, insofar as the law prohibits erasure, erasure would impair legitimate interests of the Data Subject, erasure is not possible without disproportionate effort due to the specific type of storage; or if the Data Subject disputes that the data are correct and it cannot be ascertained whether they are correct or incorrect.

3.13 Notification of Correction

If Personal Data are corrected, the Data Controller must notify any transferee of the data that it has been corrected.

3.14 Proportionality

This Policy will be applied in a reasonable manner with cost and effort proportionate to the importance of the proposed processing and the sensitivity of the data at issue.

4.0 Notification to Data Privacy Authorities Regarding Visteon's Processing Activities

Visteon shall not process Personal Data without notification to the data protection authorities in jurisdictions which require such notification. The Office of Data Protection shall keep the notifications up to date at all times.

5.0 Use of Third Party Data Processors.

5.1 Requirements for Third Party Processors.

Where the Company relies on others to assist in its processing activities, the Company will choose a Data Processor who provides sufficient security measures and take reasonable steps to ensure compliance with those measures.

5.2 Written Contracts for Third Party Processors.

Visteon shall enter into a written contract with each data processor requiring it to comply with data privacy and security requirements imposed on Visteon under local legislation.

5.3 Audits of Third Party Processors.

As part of Visteon's internal data auditing process, Visteon shall conduct regular checks on processing by third party data processors, especially in respect of security measures.

6.0 Notice to Directors, Managers, and Officers of Potential Sanctions for Non-Compliance

The Office of Data Protection shall notify directors, managers, and other officers of Visteon that: i) failure to comply with relevant data protection legislation may trigger criminal and civil liability, including fines, imprisonment, and damage awards; and ii) they can be personally liable where an offense is committed by Visteon with their consent or connivance, or is attributable to any neglect on their part.

7.0 Data Security

7.1 Physical, Technical and Organizational Security Measures

7.1.1 The Company shall adopt physical, technical, and organizational measures to ensure the security of Personal Data, including the prevention of their alteration, loss, damage, unauthorized processing or access, having regard to the state of the art, the nature of the data, and the risks to which they are exposed by virtue of human action or the physical or natural environment.

7.1.2 Adequate security measures should include all of the following:

7.1.2.1 Entry Control: Prevention of unauthorized persons from gaining access to data processing systems in which Personal Data are processed.

7.1.2.2 Admission Control: Prevention of data processing systems from being used by unauthorized persons.

7.1.2.3 Access Control: Preventing persons entitled to use a data processing system from accessing data beyond their needs and authorizations. This includes preventing unauthorized reading, copying, modifying or removal during processing and use, or after storage.

7.1.2.4 Disclosure Control: Ensuring that Personal Data in the course of electronic transmission during transport or during storage on a data carrier cannot be read, copied, modified or removed without authorization, and providing a mechanism for checking to establish who is authorized to receive, and who has received, the information.

7.1.2.5 Input Control: Ensuring that it can be subsequently checked and established whether and by whom Personal Data have been entered into, modified on or removed from data processing systems.

7.1.2.6 Job Control: Ensuring that in the case of commissioned processing of Personal Data, the data can be processed only in accordance with the instructions of the Data Controller.

7.1.2.7 Availability Control: Ensuring that Personal Data are protected against undesired destruction or loss.

7.1.2.8 Use Control: Ensuring that data collected for different purposes can and will be processed separately.

7.1.2.9 Longevity Control: Ensuring that data are not kept longer than necessary, including by requiring that data transferred to third persons be returned or destroyed.

7.2 Employee Confidentiality Agreements.

All persons involved in any stage of processing Personal Data should explicitly be made subject to a requirement of secrecy which should continue after the end of the employment relationship.

8.0 Dispute Resolution

8.1 Employees.

8.1.1 Employees with inquiries or complaints about the processing of their Personal Data should first discuss the matter with their immediate supervisor. If the Data Subject does not wish to raise an inquiry or complaint with an immediate supervisor, or if the supervisor and the Data Subject are unable to reach a satisfactory resolution of the issues raised, the employee should bring the issue to the attention of the Office of Data Protection in writing.

8.1.2 If the issue cannot be resolved through consultation with the employee's supervisor or the Office of Data Protection, it shall be handled as follows:

8.1.2.1 Through the Collaborative Resolution Procedure where applicable, or such other non-judicial procedures established by applicable employment agreements, union

agreements, or statutory provisions, as may be applicable to a particular person.

8.1.2.2 In the case of human resources data pertaining to employees in the European Union, an employee who is not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union) shall be directed to the state or national data protection or labor authority in the jurisdiction where the employee works.

8.1.2.3 Any disputes concerning the transfer of EU Personal Data to the United States pursuant to the Safe Harbor mechanism shall be resolved in cooperation with the European Data Protection Authorities as set forth in the Safe Harbor FAQs 5 and 9. These are available at the U.S. Department of Commerce: http://www.export.gov/safeharbor/sh_historicaldocuments.html. Visteon has committed to cooperate in the investigations by and to comply with the advice of competent EU authorities in such cases where the Data Protection Authority takes the view that the Company needs to take specific action to comply with the Safe Harbor Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the Data Protection Authorities with written confirmation that such action has been taken.

8.2 Non-Employees.

Non-employees with inquiries or complaints about the processing of their Personal Data should bring the matter to the attention of the Office of Data Protection in writing. Any disputes concerning the processing of the Personal Data of non-employees will be resolved through arbitration. If the dispute involves the processing of Personal Data which is not EU Personal Data, then the dispute shall be resolved by and pursuant to the rules of the American arbitration Association (“AAA”), or such other independent arbitration body as Visteon and the complaining person may agree.

8.3 Appeals.

If the issue is not resolved through consultation with the Data Subject’s supervisor or the Office of Data Protection, or through other mechanisms under existing employment agreements, union agreements, or statutory procedures, then the Data Subject may, at its option, seek redress through resort to mediation, binding arbitration, litigation, or complaint to a data protection authority with jurisdiction (all as permitted by applicable local law or procedure).

8.4 Transfers of Data from the European Economic Area to the United States.

If a matter in dispute relates to whether transfers of data from the European Economic Area to the United States have been done in

compliance with the requirements of the U.S. Safe Harbor Provisions, then such disputes shall be brought to the attention of the Office of Data Protection. The Office of Data Protection shall make an independent investigation and evaluation of the Data Subject's complaint. If the matter is not resolved to the Data Subject's satisfaction through this mechanism, the matter shall be resolved in accordance with the provisions of the Safe Harbor mechanism with enforcement by the U.S. Federal Trade Commission, as provided by the Safe Harbor provisions. This shall apply to all types of data including, without limitation, employee data.

9.0 Training.

Each Business Unit will provide training to teach, or re-emphasize privacy and security related procedures. These procedures should be set forth in written guidelines to employees and shall include at least the following:

- Each employee's duty to use and permit the use of Personal Data only by authorized persons and for authorized purposes;
- The Data Protection Principles set forth in Section 3.2;
- The contents of this Policy;
- The relationship between this Policy and other Visteon policies, including without limitation those identified in Section 10.2;
- The need for and proper use of the forms and procedures adopted to implement this Policy;
- The correct use of passwords, security tokens and other access
- mechanisms;
- The importance of limiting access to Personal Data, such as by using
- password protected screen savers, logging out when the information is not being used and attended by an authorized person;
- Securely storing manual files, print outs and electronic storage media;
- A general prohibition on the transfer of Personal Data outside of the internal network and physical office premises;
- Proper disposal of confidential data by shredding, etc.;
- Special risks associated with particular activities.

10.0 Special Rules for Specific Countries.

10.1 Country Specific Rule.

The Office of Data Protection may publish guidelines that apply in specific countries.

10.2 Integration with Other Visteon Policies.

Where Visteon has issued other policies specifically applicable to particular countries or locations, those policies shall take precedence over this Policy.

10.3 Limited Effect of Policy.
This Policy shall not be interpreted or construed as giving any individual rights greater than those which such person would be entitled to under applicable law and other binding agreements.

11.0 Compliance Measurement.

11.1 Current Compliance Assessment.
The Office of Data Protection shall establish a schedule for and implement a data protection compliance audit for all business units. The Office of Data Protection, in cooperation with the business units, shall devise a plan and schedule for correcting any identified deficiencies within a fixed, reasonable time.

11.2 Annual Data Protection Audit.
Each business unit shall review annually its data collection, processing, and security practices. This annual review shall consist of at least the following:

11.2.1 The business unit shall determine what Personal Data the business unit is collecting, or intends to collect, the purposes of the data collection and processing, any additional permitted purposes, the actual uses of the data, what disclosures have been made about the purposes of the collection and use of such data, the existence and scope of any Data Subject consents to such activities, any legal obligations regarding the collection and processing of such data, and the scope, sufficiency, and implementation status of security measures.

11.2.2 The business unit shall determine what Personal Data it has in manual systems that constitute “relevant filing systems.”

11.2.3 The business unit shall identify all transferees of Personal Data in its possession or control. The business unit shall determine where the transferee is located, the purposes of the transfer, what physical, technical, and procedural systems are in place to maintain at least the existing level of data protection and to prevent or control further transfers.

11.2.4 The information collected in this annual review shall be delivered to the Office of Data Protection for review and appropriate action including, without limitation, the following:

- Making recommendations for improvement to policies and procedures in order to improve compliance with this policy and applicable law.
- Satisfying the requirements for self-certifying compliance with the U.S. Safe Harbor provisions for transfer of Personal Data from the European Economic Area to the United States, and completing the annual recertification process under the Safe Harbor mechanisms.

12.0 Implementation.

12.1 Publication.

This Policy shall be available to employees through the Human Resources Department and shall be made available to non-employees through posting to www.Visteon.com or, posting to an alternate internet site or other means of notification as the Office of Data Protection may deem appropriate.

12.2 Effective Date.

This Policy is adopted as of March 1, 2004. The Office of Data Protection, in cooperation with the Business Units, will develop a timeline and program for implementing this Policy. This implementation program will include the resolution of any conflicts between this Policy and other existing policies.

12.3 Revisions.

This Policy may be revised at any time. Notice of significant revisions shall be provided to employees through the Human Resources Department and to others through an appropriate mechanism selected by the Office of Data Protection.

13.0 Sponsor.

The Sponsors of this Policy are the Corporate Transactions and Legal Affairs Department and the Office of Data Protection. The Office of Data Protection is responsible for maintenance and accuracy of this Policy. Any questions regarding this Policy should be directed to the Office of Data Protection.

14.0 Custodian.

The custodian of this Policy is the Office of Data Protection. Each business unit manager is responsible for implementation of the Policy. Any questions regarding the implementation of this Policy should be directed to the Office of Data Protection.

15.0 Severability.

Whenever possible, each Section of this Policy shall be interpreted in a manner as to be valid under applicable law, but if any provision shall be held to be prohibited or invalid, such provision shall be ineffective only to the extent of such prohibition or invalidity, without invalidating the remainder of such provision or the other remaining provisions of this Policy.

16.0 Other Visteon Policies

Visteon Information Security Compliance Policy

Visteon Access Control Policy

Visteon E-mail/Technology Usage Policy

Visteon Internet Access Policy

Data Processing Assessment Form

Record Retention Policy

Collaborative Resolution Procedure

17.0 Glossary

17.1 **Consent** means “any freely given specific and informed indication of his wishes by which the Data Subject signifies agreement to Personal Data relating to him being processed.”

The word “signifies” means that there must be some active communication between the parties. Thus, a mere non-response to a communication from Visteon cannot constitute consent.

Nevertheless, consent may be obtained by a number of methods. These may include clauses in employment contracts, check boxes on replies to application or purchase forms, and click boxes on online forms where Personal Data are entered.

In most European Union countries, consent to the processing of Sensitive Personal Data needs to be clear and unequivocal. This generally means that some form of specific, active consent (See Section 17.7 “opt-in” consent) is required. There is greater divergence in national approaches when it comes to deciding what constitutes consent for processing other types of Personal Data. Some jurisdictions take a less restrictive approach, and will accept the concept of implied consent (See Section 17.8 “opt-out” consent) in limited circumstances. For purposes of Visteon’s compliance, and in the interest of a uniform Policy that will be acceptable in all countries outside the United States, Visteon will follow the “opt-in” form of affirmative consent.

Consent is limited to the specific purposes disclosed to the individual. Further notification and consent is required for new processing activities that extend beyond those for which consent was originally obtained. In the context of new data aggregating activities for which consent had not previously been obtained, additional consent is required. Thus, if data that was collected under an original consent is later aggregated with other data for purposes of transferring the aggregated data to third parties and/or overseas, the original consent likely did not cover this latter activity, requiring additional consent specific to the new uses of the data.

In the case of Sensitive Data, all European laws agree on an opt-in approach. The Data Subject’s consent must be communicated to Visteon *before* any processing can take place, unless an exception applies. These include the processing of data mandated by employment law, cases in which it is impossible for the Data Subject to consent, and where the data to be processed is public information or information manifestly intended to be made public. Individual countries may provide for additional exceptions for reasons of substantial public interest.

Any processing of sensitive Personal Data not needed for the proper business operations of Visteon must be terminated.

17.2 **Data** (whether or not having an initial capital letter) as used in this Policy shall mean information which either:

- is being processed by means of equipment operating automatically in response to instructions given for that purpose;

- is recorded with the intention that it should be processed by means of such equipment;
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;
- does not fall within any of the above, but forms part of a readily accessible record covering an individual.

Data therefore includes any digital data by computer or automated equipment, and any manual information which is part of a relevant filing system.

17.3 **Data Controller** means a person who (alone or with others) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed. Generally, Visteon itself will be the Data Controller, although there may be more than one Data Controller within a group of companies if local or overseas offices, subsidiaries or affiliates within the group enjoy a level of autonomy over the processing of the Personal Data they use.

17.4 **Data Processor** means any person, other than an employee of the Data Controller, who processes the data on behalf of the Data Controller.

17.5 **Data Subject** means the person to which data refers. Data Subjects include customers and web users, individuals on contact /e-mailing lists or marketing databases, employees, contractors and suppliers.

17.6 **EU Personal Data** means Personal Data which are collected or processed by an entity established in a European Union Member State, or which were processed on equipment located in a European Union Member State, except for processing which consists solely of transmitting Personal Data.

17.7 **Opt-in** refers to a system whereby Data Controllers obtain specific consent from the Data Subject before the Data Subject's personal information is processed or otherwise used for a particular purpose.

17.8 **Opt-out** refers to a system whereby Data Controllers deem consent to have been given unless a Data Subject specifically refuses to have their Personal Data processed or otherwise used for a particular purpose by the Data Controller.

17.9 **Personal Data** means data related to a living individual who can be identified from those data or from those data and other information in the possession of, or likely to come into the possession of, a Data Controller or Data Processor.

17.10 **Processing** covers a wide variety of operations relating to data, including obtaining, recording or holding the data or carrying out any operation or set of operations on the data, including:

- Organization, adaptation, or alteration;
- Disclosure by transmission, dissemination, or otherwise; and
- Alignment, combination, blocking, erasure, or destruction.

17.11 **Relevant Filing System** means any set of information relating to individuals, whether kept in manual or electronic files, structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Therefore any digital database and/or organized manual files relating to identifiable living individuals fall within the scope of data protection laws and regulations, while a database of pure statistical or financial information (which cannot either directly or indirectly be related to any identifiable living individuals) will not.

17.12 **Sensitive Data** means Personal Data containing information as to the Data Subject's:

- Race or ethnic origin;
- Religious beliefs or other beliefs of a similar nature;
- Political opinions;
- Physical or mental health or condition;
- Sexual history or orientation;
- Trade union membership;
- Commission or alleged commission of any offense and any related court proceedings.

17.13 **Technology** is to be interpreted broadly, to include any means of collecting or processing Data, including, without limitations, computers and networks, telecommunications systems, video and audio recording devices, biometric devices, closed circuit television, etc.

17.14 **United States** means the 50 states of the United States of America and all its territories, possessions, and mandates, including without limitation Guam, the District of Columbia, and the Commonwealth of Puerto Rico.

18.0 Exhibits

18.1 Exhibit A – Office of Data Protection

EXHIBIT A

Office of Data Protection as of April 2013

Chief Compliance Officer:	Michael K. Sharnas One Village Center Drive Van Buren Twp., MI 48111 E-mail: msharnas@visteon.com Voice: (734) 710-5236 Fax: (734) 736-5560
Data Protection Officer – U.S.	Janet Witkowski One Village Center Drive Van Buren Twp., MI 48111 E-mail: jwitkow4@visteon.com Voice: (734) 710-5265 Fax: (734) 736-5560
Data Protection Officer – Europe and South America	Gregor Scheja Visteonstrasse 4-10 D-50170 Kerpen Germany E-Mail: gscheja@visteon.com Voice: +49-2273-595-2465 Mobile: +49-0172-432-1777 With regard to activities subject to the German Federal Data Protection Act, the Data Protection Officer – Europe shall be directly subordinate to the head of the Visteon entity or entities established in Germany.