

08.10.2018

# **Delphi** **Technologies**

## **Privacy Policy**

At Delphi we take privacy and confidentiality matters very seriously. We have developed this privacy policy (hereinafter the “**Privacy Policy**”) to clearly define our ongoing commitment to protecting privacy rights and to guide how we collect, use and disclose the personal information as required by applicable law or as we require in the course of fulfilling our professional responsibilities and operating our business.

This Privacy Policy is issued by Delphi Powertrain Systems Operations Luxembourg S. à r.l., a *société à responsabilité limitée* formed under the laws of Luxembourg, with registered offices at Avenue de Luxembourg, L- 4940 Bascharage, Grand Duchy of Luxembourg, registered within the *Registre de Commerce et des Sociétés* in Luxembourg under the number B215656. It applies to all subsidiaries and affiliates of the Delphi Group located within the European Union. These subsidiaries and affiliates each act as Controller (as defined below) in relation to the processing of the Data Subjects’ Personal Data they perform (as defined below). References to “**Delphi**”, “**we**” or “**us**” in this Privacy Policy include all such subsidiaries and affiliates.

## 1. Definitions

The terms and expressions in capital letters used in the Privacy Policy have the meanings set forth below. Words in singular include the plural and vice versa. These terms and expressions shall always be interpreted according to applicable data protection rules including, but not limited to, the European Union Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the “**Data Protection Legislation**”).

“**Controller**”: means a Delphi entity which determines the purposes and the means of Personal Data processing.

“**Data Subjects**”: means natural persons whose personal data is being processed by Delphi.

“**Personal Data**”: means any information allowing the direct or indirect identification of an individual.

“**Sensitive Data**”: means Personal Data revealing directly or indirectly the racial or ethnic origin, political, philosophical or religious opinions, trade union affiliation, or related to the health or sexual life of Data Subjects.

“**Technical and Organizational Security Measures**”: means measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of Personal Data over a network, and against all other unlawful forms of processing.

## 2. Collection of Personal Data

**When does Delphi collect your Personal Data?** Delphi may collect and store, in accordance with Data Protection Legislation, some Personal Data from Data Subjects having interactions with Delphi. Data Subjects may include, but are not limited to:

- employees, interns, temporary workers, directors, shareholders, and job applicants (i.e. individuals seeking employment with Delphi);
- investors;
- external consultants;
- visitors of the Delphi premises;
- third party providers;
- clients / customers of Delphi.

**Types of Personal Data.** Personal Data collected and stored by Delphi may include, but are not limited to, the following types of data:

- identification data (such as name, family name, date of birth, gender);
- contact information (such as phone numbers, email address, mailing addresses);
- other relevant personal details (nationality, citizenship, marital status, other family-related data, company name, role/function);
- government identification numbers (social security numbers, tax payer ID's, driver's license, etc.);
- HR related data such as time of attendance, trainings and professional qualifications, benefits, salaries, etc.;
- types of services received or products bought;
- financial and banking information (notably linked to remuneration);
- pictures and sound;
- footage from video surveillance;
- log data of entry and exit to and from the premises and vehicle information (e.g. licence plate number);
- any other Personal Data reasonably related to the conduct of Delphi's business.

There may be instances in which the Personal Data that a Data Subject provided to us is considered as Sensitive Data under local data protection laws.

Most of the Personal Data we process is information that is knowingly provided to us. However, please note that in some instances, we may process Personal Data received from a third party with their knowledge.

**Purpose of the processing of Personal Data.** Personal Data shall mainly be processed for the following purposes:

- administration of the staff and external consultants;
- management of human resources;
- management of the payroll;
- accountancy;
- management of third party providers;
- management of visitors;
- management of clients/customers;
- management of litigation;
- management or implement any business reorganisation including in the form of a disposal, merger or acquisition, sale or transfer of business or assets;
- monitoring of information and communications systems to the extent and for the purposes permitted under applicable law.

No automated decisions will be made in relation to the Personal Data processed.

Delphi makes sure that only the Personal Data that are necessary to achieve the above-listed purposes are processed.

The collection of Personal Data is legitimate because such Personal Data are mainly necessary for the purpose of the legitimate interests pursued by Delphi, for the performance of contractual obligations and/or for Delphi to comply with its legal obligations.

Indeed, the processing of Personal Data performed by Delphi is necessary for Delphi to carry out its daily activities, that is to say, but is not limited to, managing its employees, providing the services required by its customers, interacting with and managing third party providers and visitors as well as complying with contractual and legal obligations related thereto.

**Update of Personal Data.** Delphi will endeavour to keep the Personal Data in our possession or control accurate. Individuals providing Personal Data are therefore responsible for promptly informing Delphi of any change to their Personal Data.

### 3. Disclosure of Personal Data

Personal Data will not be shared with third parties, except as provided below.

**Disclosure of Personal Data.** We may disclose Personal Data to the following categories of recipients:

- external services providers;
- professional advisors;
- public authorities and administrations;
- customers / clients of Delphi;
- affiliate companies of Delphi.

Delphi may disclose Personal Data in the following circumstances:

- in the event of a legal request and/or investigation when, in our opinion, such disclosure is necessary to prevent crime or fraud, or to comply with any statute, law, rule or regulation of any governmental authority or any order of any court of competent jurisdiction;
- if we outsource some or all of the operations of our business to third party service providers, as we do from time to time. In such cases, it may be necessary for us to disclose Personal Data to those service providers. Sometimes the service providers may process some Personal Data on behalf of and under the instructions of Delphi. We restrict how such service providers may access, use, disclose, and protect that data;
- in case of business transfers in the event of the sale or acquisition of companies, subsidiaries, or business units. In such transactions, Personal Data may be part of the transferred business assets but remain subject to the protections in any pre-existing privacy statement;
- when we believe release is appropriate or necessary to conduct the company's business, comply with the law, enforce or apply our policies and other agreements, or protect the rights, property, or safety of Delphi, our employees, or others.

In such circumstances, Delphi ensures that Personal Data is kept secure from unauthorized access and disclosure.

**Transfer of Personal Data within the Delphi group.** Being a global company operating worldwide, Delphi processes Personal Data in several countries and from different origins, and transfers data all over the globe. Delphi is sharing data in the normal course and scope of business with other affiliated companies, as well as third parties.

Data Subjects are informed that certain recipients may be located outside the territory of the European Union and in countries that do not offer a level of protection equivalent to the one granted in the European Union.

In this respect, Delphi has taken appropriate guaranties and concluded the necessary agreements to ensure complete security of the Personal Data transferred. Copies of existing agreements can be provided upon written request at [personaldata.informationrequest@delphi.com](mailto:personaldata.informationrequest@delphi.com).

Other transfers to external third parties located outside the European Union in countries not deemed to offer an equivalent level of protection for personal data may also be authorized by the Data Protection Legislation under a derogation relating, as the case may be, to the performance of a contract concluded in your interest or for the establishment, exercise or defence of legal claims or for the performance of a contract between you and us.

#### **4. Data Subjects' rights in relation to the processing of their Personal Data**

**Rights granted to Data Subjects.** In accordance with applicable law, Data Subjects are granted the following rights with regard to the processing of their Personal Data:

- the right to request access to the Personal Data stored by Delphi;
- the right to update or correct any of their Personal Data, if the Personal Data is incorrect;
- the right to oppose to the processing of their Personal Data, on grounds related to their particular situation;
- the right to request from Delphi the erasure of the Personal Data, to the extent such Personal Data (i) are no longer necessary in relation to the initial purpose(s) for which they were collected, (ii) consent has been withdrawn and there is no other means of legitimating the processing of Personal Data, (iii) the Data Subject objects to the processing of the Personal Data, (iv) the Personal Data is unlawfully processed;
- the right to request the restriction of the processing of Personal Data, if such Personal Data is found to be inaccurate or unlawful, is no longer needed for the purposes of the processing, or should a court decision on a complaint lodged by a Data Subject be pending;
- the right to data portability;
- the right to withdraw consent to data processing given in the context of the Data Subjects' relationship with Delphi;
- in the event of a dispute between the Data Subject and Delphi regarding the processing of Personal Data which failed to be resolved by the parties in an amicable manner, the right to lodge a complaint with the Luxembourg Data Protection Authority (the *Commission Nationale pour la Protection des Données* - CNPD). Data Subjects not residing in Luxembourg can contact their local Data Protection Authority.

Delphi will respond to individual complaints and questions relating to privacy and will investigate and attempt to resolve all complaints. Delphi undertakes to handle each request by a Data Subject free of charge and within a reasonable timeframe.

**How to exercise such rights.** Data Subjects can exercise the rights mentioned above or challenge compliance with this Privacy Policy, by contacting Delphi by email at the following address: [personaldata.informationrequest@delphi.com](mailto:personaldata.informationrequest@delphi.com).

The data protection Compliance Office will ensure that a complete investigation of all complaints has been undertaken and will report their findings to Data Subjects in most instances within ten (10) working days. In case the complaint is considered as justified, the Compliance Office will promptly inform the Data Subject that his or her complaint is accepted and will take all measures to adequately address the issue raised. In case the complaint is rejected by the Compliance Office, the Data Subjects will be promptly informed of such rejection. If the Data Subject is not satisfied with the reply given to his or her complaint by the Compliance Office, the Data Subject will be able to refer to the relevant court or to the CNPD to deal with the complaint.

#### **5. Data retention**

Delphi undertakes not to use the Personal Data for purposes other than those for which it has been collected and that such information shall not be stored for a period longer than necessary for the realization of such purposes.

Retention periods shall, in any case, be compliant with any applicable law and proportionate to the purposes of the processing.

## **6. Technical and Organizational Security Measures**

Ensuring that Personal Data is appropriately protected from data breaches is a top priority for Delphi.

Delphi implements adequate Technical and Organizational Security Measures, such as password protection, encryption, physical locks, etc., to ensure a level of security appropriate to the risks represented by the processing and the nature of the Personal Data to be protected.

Sensitive Data are processed with enhanced and specific security measures.

Access to Personal Data is permitted to employees for the sole purpose of performing their professional duties, such employees being subject to a confidentiality obligation.

## **7. Internal training program and sanctions for non-compliance**

All Delphi employees having access to Personal Data are provided with specific training programs in order to improve their practical skills and knowledge that relate to data protection issues. Privacy training programs are an integral part of professional development within Delphi.

All guidelines, procedures or policies related to the protection of Personal Data are uploaded on Delphi's corporate intranet and permanently accessible to every employee and provided to every new employee. Internal notices may also be transmitted within the Delphi Group from time to time.

Non-compliance of employees with these rules may be regarded as a serious breach of the trust Delphi must be able to place in its employees and other members of the staff. Non-compliance by an employee may therefore result in a sanction, such as suspension or other disciplinary measures or measures under labour law, which may include summary dismissal. Non-compliance by members of staff that are not employees may result in termination of the relevant contract with this member of staff.

## **8. Amendment**

Delphi reserves the right to change, supplement and/or amend this Privacy Policy at any time.

In such case, notification will be given through our intranet and/or by email, or any other methods allowed by Data Protection Legislation.

## **9. Contact**

Delphi has set up a Compliance Office in order to manage and monitor global compliance for Delphi to data protection obligations.

This Compliance Office is composed as follows:

- Global Data Privacy Officer:  
Isabelle Vagne, Regional General Counsel and Compliance Officer EMEA  
Email: [Isabelle.Vagne@delphi.com](mailto:Isabelle.Vagne@delphi.com)  
Tel. +33 (0) 1 70 76 72 62

## **Delphi** Technologies

- Authorized Data Protection Compliance Manager:  
Thomas Whiteley, Attorney  
Email: [Thomas.Whiteley@delphi.com](mailto:Thomas.Whiteley@delphi.com)  
Tel. +352 5018 2277
- Local Data Protection Officers who are the HR functional leaders of each Delphi entity.

For any question or queries you may have regarding this Privacy Policy, please use the following email address: [personaldata.informationrequest@delphi.com](mailto:personaldata.informationrequest@delphi.com) or contact your HR manager locally.