

Privacy Statement for HR Personal Data of EU-based Employees under the Privacy Shield

The United States Department of Commerce and the European Commission have agreed on a set of data protection principles and frequently asked questions to enable U.S. companies to satisfy the requirement under European Union (“EU”) law that adequate protection to be given to personal information transferred from the EU or European Economic Area (“EEA”) to the United States (the “Privacy Shield” – <https://www.privacyshield.gov/>). The European Commission also has recognized the US-EU Privacy Shield as providing adequate data protection. General Cable Corporation and General Cable Industries, Inc. (together “GC”) are fully committed to the Principles of the Privacy Shield. The entire Privacy Shield List of the US Department of Commerce can be reviewed here: <https://www.privacyshield.gov/list> .

This Privacy Statement answers the following questions:

- What work-related information (Human Resource (“HR”) data) from the EU/EEA do we collect about you?
- How do we use this information?
- Will we share your personal data with third parties?
- What choices do you have about the collection and use of your personal data?
- What security measures do we take to safeguard your personal data?

IMPORTANT NOTE: For all personal data that GC receives under the Privacy Shield, GC has agreed to a Privacy Statement for Personal Data under the Privacy Shield at generalcable.com/privacy-policy. This Statement also applies to HR-related data. Please open and read this Statement carefully and contact your HR department if you have questions.

This Privacy Statement for Personal Data under the Privacy Shield addresses in particular:

- o the type or identity of third parties to which GC discloses personal information, and the purposes for which it does so
- o the right of individuals to access their personal data
- o the choices and means GC offers individuals for limiting the use and disclosure of their personal data
- o that GC is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC)
- o the possibility, under certain conditions, for the individual to invoke binding arbitration
- o the requirement for GC to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and

- o GC's liability in cases of onward transfers to third parties.

In addition to this Statement, for HR or employee personal data that GC receives under these Privacy Shield Principles from its affiliated companies and their providers, the following rules apply:

Additional Privacy Shield Requirements for HR (Employee) Data

(1) Coverage by the Privacy Shield

GC processes any of the following personal data sets from its EU-based **employees and job applicants**:

- Identification details. For example: name, passport/personal identification number or similar document, work/home address, work/home telephone, e-mails addresses, age, gender, date of birth, social security number, current marriage and details of their family.
- Education and training details. For example: academic records, qualifications, skills, training records, professional expertise, positions held with previous employers.
- Employment and financial details. For example: information on employee organizational assignment, such as type of employment, payroll accounting area, job function, information on global assignment and expatriate status, type of compensation, annual salary, travel expenses, details of bank to which payment is made (bank account, address and country of the bank and so on), pay-scale type, rewards and recognition details data related to pensions and other benefit programs.
- Operational details. For example: Account user name /passwords.
- Information related to compliance programs: Information submitted by individuals regarding conflict interest monitoring, ethic/help line internal program and other compliance issues.

These HR personal data sets are processed by GC for any of the following purposes:

- (i) Defining employees' assignment to functions, keeping track of staffing, and working time planning;
- (ii) Internal compensation, benefits, bonus and long term incentive pay calculations and planning;
- (iii) Travel and emergency tracking;
- (iv) A worldwide web-based recognition and rewards program;
- (v) A worldwide benefits program;
- (vi) Performance management;
- (vii) Talent and organizational design and development,
- (viii) Compliance of internal policies, code of conduct, whistleblowing mechanism, and similar programs,
- (ix) IP rights/ patent management and internal awards program, and

(x) Recruitment of employees.

Please note the following restrictions and clarifications:

- All these data sets can be transferred and processed by so called agents (service providers of GC) under the conditions and within the limits of GC's general Privacy Shield Statement.
- The Privacy Shield Principles are relevant only when individually identified or identifiable data are transferred or accessed.
- GC receives these data sets from its subsidiaries or affiliate in the EU for the aforementioned purposes. These data transfers are fully covered by the Privacy Shield. The collections and other processing of the personal data and its processing prior to transfer have been subject to the national laws of the EU Member State where they were collected. This means that GC and its agents will respect the conditions for the processing or restrictions on its transfer according to those laws.

(2) Application of the Notice and Choice Principles

(i) Once GC or its agents have received employee data under the Privacy Shield Principles from the EU, they may disclose it to third parties or use it for **different purposes** only in accordance with the GC's Privacy Shield Statement generalcable.com/privacy-policy. For example, where GC intends to use personal data collected through the employment relationship for non-employment-related purposes, such as marketing communications, GC must first provide the affected employees with the necessary choice before doing so (opt-in). GC will contact you when such an opt-in will become necessary. Such choices will never be used by GC to restrict employment opportunities, to discriminate or take any punitive action against such employees.

(ii) GC makes a reasonable effort to accommodate employee privacy preferences. This effort could include, for example, restricting access to the personal data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purposes. Please contact your local HR department for more details.

(3) Application of the Access Principle

GC subsidiaries serving as employers in the EU will continue to comply with local regulations and ensure that EU employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage. GC will cooperate in providing such access either directly or through the EU employer.

(4) Enforcement

(i) In compliance with the Privacy Shield Principles, GC commits to resolve complaints about our collection or use of your personal information. Individuals in the European Union (EU) with inquiries or complaints regarding our Private Shield policy should first contact their local HR departments. . Where EU-based employees raise complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they can address their complaint with the state or national data protection or labor authority in the jurisdiction where they work, according to applicable law. (ii) To the extent that GC uses HR or employment personal data transferred from the EU in the context of the employment relationship being covered by the Privacy Shield, GC has

committed to cooperate with EU data protection authorities (DPAs) with regard to unresolved Privacy Shield complaints. If you do not receive timely acknowledgment of your complaint from us, or if we have not addressed your complaint to your satisfaction, please contact the EU DPAs for more information or to file a complaint. The services of EU DPAs are provided at no cost to you.

(5) Application of the Accountability for Onward Transfer Principle

GC uses agents for the data collections and processing described in Section 1.

As foreseen by the Privacy Shield Principles, there may be occasional employment-related operational needs of GC to process certain employee data transferred under the Privacy Shield, such as the booking of a flight, hotel room, or insurance coverage, transfers of personal data of a small number of employees. Such processing can take place without application of the Access Principle or entering into a contract with the third party, as otherwise required under the Accountability for Onward Transfer Principle, provided that GC has complied with the Notice and Choice Principles.

COMPLIANCE

GC has implemented appropriate internal measures and policies to ensure that the GC employees receive training on the Privacy Shield Principles and their implementation. Employees who violate them are subject to disciplinary action.

CHANGES TO THIS STATEMENT

If there are updates to the terms of this statement, GC will post those changes here and update the revision date in this document so that you will always know what information GC collects, how we use it, and what choices you have.

CONTACT INFORMATION

Giorgio Totis

giorgio.totis@prysmiangroup.com

Postal address

General Cable Corporation, 4 Tesseneer Drive, Highland Heights, KY USA 41076-9753

Last Updated: February 7, 2019.