CORNING Global Data Privacy Policy

Version effective as of September 5, 2013

Foreword Corning[1] is the world leader in specialty glass and ceramics. We create and make keystone components that enable high-technology systems for consumer electronics, mobile emissions control, telecommunications and life sciences. As part of our business operations, we collect and process relevant Personal Data[2] about our employees, applicants, contractors, customers, suppliers and other business partners.

Purpose The purpose of this Policy is to describe the standards that Corning applies when it processes Personal Data. It outlines in particular the type of Personal Data that Corning processes, how it uses such Data, and what are the rights of the individuals whose Data is concerned and how they can exercise those rights. The objective of this Policy is to provide adequate protection for the transfers and processing of Personal Data by the Corning Group.

Scope This Policy covers all Personal Data processed by or on behalf of any Corning entity, irrespective of the format of such Data (e.g. electronic records, manual (paper-based) files, recordings, conversations, disks).

Intended Audience All Corning entities and all Corning employees are required to comply with this Policy. Any third parties entrusted with Personal Data by or on behalf of Corning must provide satisfactory assurances of Data protection standards that are at least equivalent to those contained in this Policy.

Safe Harbor Corning US entities adhere to the US - EU Safe Harbor Framework and to the US - Swiss Safe Harbor Framework regarding the transfer of Personal Data from the European Union and Switzerland to the United States of America. Accordingly, Corning US entities follow the Safe Harbor Principles published by the US Department of Commerce with respect to such Data (Notice; Choice; Onward Transfer; Access; Security; Data Integrity; Enforcement). To learn more about the Safe Harbor program, and to view Corning's certification, please visit **http://www.export.gov/safeharbor/**.

Publication Corning commits to make the present Policy readily available to every Data Subject. To this purpose, the current version of this Policy is posted on Corning's intranet and Corning's external website.

GENERAL RULE

Corning is committed to protecting and safeguarding the Personal Data entrusted to it by its employees, customers, suppliers, business partners and others with whom it interacts.

---

[1] Corning (or Corning Group, we, our) – refers to Corning Incorporated (with its principal place of business at 1 Riverfront Plaza, Corning, NY, 14831, USA) and to its direct and indirect majority-owned subsidiaries.

2 The term "Personal Data" or "Data" means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. This term and any other capitalized term shall be interpreted according to the EU Directive 95/46/EC which shall prevail over the definitions provided in this Policy in case of discrepancy. If and to the extent national data protection laws are applicable that also protect information relating to identified or identifiable *legal entities*, the term "Personal Data" shall also include such information.

Corning's Data protection practices and programs are aligned with Corning's Values and applicable laws and regulations. Corning requires its business partners to uphold at least as stringent Data protection practices for the Personal Data entrusted to them.

DATA PROTECTION PRINCIPLES

This Policy reflects the following fundamental Data protection principles that Corning entities observe and according to which Personal Data is:

- Consistent with the Notice, Choice and Access Safe Harbor Principles,
  - Processed fairly and lawfully;
  - Collected for specified, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes;
  - Processed in accordance with the Data Subject's rights;
- Consistent with the Data Integrity Safe Harbor Principle,
  - Adequate, relevant and not excessive in relation to the purposes for which it has been collected and/or further processed;
  - Accurate and, where necessary, kept up to date;
  - Stored for no longer than necessary for the purposes for which it has been collected and/or further processed;
- Consistent with the Security Safe Harbor Principle,
  - Processed using adequate security and confidentiality measures; and
- Consistent with the Onward Transfer Safe Harbor Principle,
  - Not transferred (or further transferred) unless an adequate level of Personal Data protection is in place.

1. Lawful and Fair Processing

Corning collects and processes[3] Personal Data in a fair and lawful manner, to the extent necessary for its legitimate business interests, and in consideration of the rights of the individuals, including without limitation the right to be informed about the Data collected and held about them. Corning provides timely Notice and Choice to Data Subjects.

Notice – Notice refers to the information that a Data Subject has the right to receive regarding the processing of his/her Personal Data, i.e. the name and contact details of the Data Controller[4], the purposes for which Corning uses the individual's Personal Data, and any additional information to the extent it is necessary, having regard to the specific circumstances in which the Data are collected, to guarantee a fair processing in respect of the Data Subject.

[3] Processing (of Personal Data) means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

[4] Data Controller or Controller means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data.

If the Data will be transferred to other countries that do not afford the same level of privacy and security protection as the originating country, that information will also be included in the Notice, along with information relating to how the Data Controller will ensure an adequate level of protection for the Data.
Where the Data have not been obtained from the Data Subject, the obligation to inform the Data Subject does not apply if (i) the provision of such information proves impossible, or (ii) would involve a disproportionate effort or (iii) recording or disclosure of such Data is expressly required by law.

Choice - Data Subjects may oppose at any time to the processing of their Personal Data, on compelling legitimate grounds relating to their particular situation, unless that processing is required by applicable law. Where the objection is justified Corning will stop the processing and delete the Data from its system, and instructs its Data Processors[5] to do the same.

2. Specified, Explicit and Legitimate Purposes – Without Further Processing
Corning processes Personal Data for specified, explicit, and legitimate purposes and does not further process the Data in a way that is incompatible with those purposes. If Corning seeks to use Personal Data for a purpose that was not identified to the Data Subject at the time the Data was collected, Corning will provide Notice to the Data Subject prior to engaging in that secondary use.

3. Adequate, Relevant and Not Excessive
Corning limits the collection of Personal Data to that which is appropriate and proportionate for its business purposes. The specific types of Data that are collected for a particular program may vary, depending upon the reason for collection and applicable regulations. If Corning receives Personal Data that is excessive or irrelevant for the intended purpose of collection, or beyond the scope of the Data Subject's Notice, Corning shall, as may be warranted, take steps to prevent future excessive or irrelevant transmissions of Personal Data from the sender, and shall use reasonable means (such as destruction) to ensure that the irrelevant or excessive Personal Data is not further processed.

4. Accurate and Kept Up to Date
Corning takes appropriate steps to ensure that the Personal Data it processes is accurate, and where necessary, corrected and kept up to date. Data Subjects may contact the Corning Point of Contact identified in the relevant section below. Where possible, Corning also provides individuals with automated means to access, correct and/or update their Personal Data.

5. Appropriate Data Retention
Corning retains Personal Data consistent with legal and business retention requirements, and does not store Personal Data when it is no longer relevant for the purposes for which it has been collected. When the maximum retention period required by applicable law or the retention period required for the purpose of collection (whichever date occurs later) is reached, Corning takes reasonable steps to destroy the Personal Data.

6. Right of Access, Rectification, Erasure and Blocking of the Personal Data
Subject to the limitations identified in applicable Data protection laws, Data Subjects may request information about the Personal Data relating to them contained in Corning's files, the purpose of Data processing, the recipients of the Data and the scope of access they have been granted. Legitimate and reasonable access requests will be responded to promptly and in any event, where applicable, within the time allowed by applicable national legislation.
Each Corning entity may decide to charge a fee for such access requests; such fee may not be excessive and may be subject to limitation by applicable local laws.

---

[5] Data Processor or Processor means a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the Controller. The equivalent term under Safe Harbor terminology is Agent – an Agent is a third party that is acting as agent to perform tasks on behalf of and under the instructions of the Controller.

If any Personal Data is inaccurate or incomplete, the individual may request that such Data be amended. It is every Corning employee's responsibility to provide Human Resources with accurate Personal Data about him or her and to inform Human Resources of any changes. To the extent appropriate, Corning will amend, rectify or erase the Data at issue, and inform any Data Processors who have received such Data from Corning to amend, rectify or erase it accordingly.

7. Adequate Security and Confidentiality Measures

Corning has put in place appropriate and commercially reasonable technical, organizational and physical security measures to keep Personal Data that it collects and holds confidential and protect it against unauthorized or unlawful disclosure or access, accidental loss, destruction, alteration or damage. These measures are intended to ensure an appropriate level of security in relation to the risks inherent to the processing and the nature of the Personal Data to be protected, in a manner consistent with the security requirements contained in the applicable Data protection law.

Corning takes appropriate measures to ensure that third parties who are given access to Personal Data reasonably uphold at least as stringent security measures as those applied by Corning.

8. Transfers to Third Parties and/or to Third Countries

Corning is a global organization, with legal entities on the five continents, and businesses, IT systems, management structures and processes that cross borders. As such, it is sometimes necessary for Corning to transfer Personal Data to other Corning entities or to third parties, in the same country as or in countries other than the country in which it was initially provided, and/or store Personal Data in databases that may be hosted in or accessible from other countries.

Transfers to Corning entities: Transfer of Personal Data from one Corning entity to another Corning entity shall be allowed only if the transfer is based on a specific and legitimate business purpose, and the receiving entity ensures compliance with this Policy and with any stricter local laws applicable to the transfer and to any subsequent processing (including onward transfer). Written agreements may be concluded where required.

Transfers to entities outside of the Corning Group:

- Selected Third Parties: Corning has entered or will enter into appropriate written agreements with third party service providers to ensure that they process Personal Data in accordance with Corning's instructions, and set up and maintain appropriate security and confidentiality measures to ensure an appropriate level of protection.

In addition, Corning will require from such third parties satisfactory assurances (i) of standards which are at least equivalent to those contained in this Policy (ii) and of compliance by the third party with applicable Data protection laws, in particular those applying to the transfer of Data and to any onward transfers. Such selected third parties will have access to Personal Data solely for the purposes of performing the services specified in their applicable service agreements. If a Corning entity concludes that a service provider is not complying with these obligations, it will promptly take appropriate actions.

- Other Third Parties: Corning entities may be required to disclose certain Personal Data to other third parties. In particular, such disclosure may be required to comply with applicable laws (e.g. disclosure of salary Data to tax authorities) or when the health or security of a Data Subject is endangered (e.g. in case of an accident). Corning may also disclose Personal Data to protect its legal rights (e.g. in a litigation).

9. Processing of Sensitive Data

Sensitive Personal Data means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, data concerning health, sex life or sexual orientation, and data relating to offences, criminal convictions or security measures.

Corning does not process Sensitive Personal Data unless:

- The Data Subject has given his/her explicit consent to the processing of those sensitive Data (except where the applicable laws prohibit it); or

- The processing is necessary for the purposes of carrying out the obligations and specific rights of the Corning entity acting as Data Controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
- The processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his/her consent; or
- The processing of Sensitive Personal Data is necessary for the establishment, exercise or defense of legal claims.

It is not anticipated that Sensitive Personal Data will be required outside of the country of origin. Any request to move Sensitive Personal Data outside of the country of origin must be approved by Corning's Data Privacy Officer.

COMMITMENT, AND MEANS IMPLEMENTED, TO COMPLY WITH THIS POLICY

Corning has set up a Data Privacy organization and maintains programs to monitor periodically adherence to this Policy and to help ensure compliance with laws, requirements and contractual agreements that apply to the Personal Data processed.
Such programs include periodical training and audits that enable Corning to verify that our Policy is accurate, comprehensive, prominently displayed, completely implemented and accessible.
Corning has appointed a Data Privacy Officer, responsible at the Corning Group level for compliance with this Policy and for initiating and coordinating any required evolution of this Policy and related policies and procedures. Corning's Data Privacy Officer reports to Corning's Chief Information Security Officer.

CLAIMS HANDLING AND ENFORCEMENT MECHANISMS

Corning entities will take appropriate remedial action, which may include disciplinary sanctions, in accordance with applicable law, if Personal Data is accessed, processed, or used in any way that is inconsistent with this Policy.

If at any time, an individual believes that Personal Data relating to him or her has been processed in violation of this Policy, he or she may report the concern to the Data Privacy Officer. All claims will be treated confidentially, and will be directed to the Data Privacy Officer, who will be in charge of coordinating the review of the claim and any investigation process pursuant to the claim. To the extent required based on the findings, the Data Privacy Officer will decide upon corrective actions, their implementation and remedy to the claim if and as appropriate.

If a complaint cannot be resolved through Corning's internal process:

- For unresolved complaints brought by an employee of a Corning entity incorporated in the European Union, Corning will cooperate with the national Data Protection Authority in the jurisdiction where the relevant Corning entity is established.
- For unresolved complaints brought by an employee of a Corning entity incorporated in Switzerland, Corning will cooperate with the Swiss Federal Data Protection and Information Commissioner.
- For other complaints, Corning agrees to dispute resolution using the American Arbitration Association as a third party resolution provider.

CORNING POINT OF CONTACT

For any questions on this Policy, or any complaints, or requests (such as access, objections or rectification requests), we encourage you to contact:

Data Privacy Officer

DTAPRIOFFC@corning.com

If you are a Corning employee, you may also contact your location's or Division's Human Resources Manager.

AMENDMENTS

This Policy may be amended from time to time. The newest version of the Policy will be posted on the intranet and extranet website and may also be distributed (in hard copy or electronic version) as appropriate to employees.