Global Data Protection Policy

Updated March 31, 2024

PREAMBLE

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. When performing our business operations, we collect and process relevant Personal Data[2] about our employees, applicants, contingent workers, customers, suppliers and other business partners.

The present policy (hereafter "Policy") sets forth CORNING's commitments regarding the protection of Personal Data. In order to ensure a maximum level of Personal Data protection, CORNING is aligned with the standards provided by the Regulation EU) 2016/679 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (hereinafter referred to as the "General Data Protection Regulation" or "GDPR").

In addition, CORNING has implemented a set of Binding Corporate Rules ("BCRs") to ensure that Personal Data is protected while transferred within the CORNING Group. The implementation of BCRs provides an adequate level of protection for the Personal Data Transfers[3] carried out from CORNING EU entities to other CORNING entities located throughout the world. The principles of the BCRs are also aligned with the GDPR. In addition to legitimizing the international transfer of Personal Data intra-group, the BCRs enable CORNING to apply a consistent and effective approach to data protection compliance throughout the world. CORNING applies the BCRs globally and in all cases where CORNING processes Personal Data. To learn more about the BCRs, please visit:

http://www.corning.com/worldwide/en/privacy-policy/binding-corporate-rules.html

CORNING has also established a privacy office (referred to as the "Corning Privacy Office" or "CPO") to facilitate global data protection compliance through adoption of

[1] "CORNING" (or "we," "our") – shall mean Corning Incorporated, a New York corporation, headquartered in Corning, NY, USA, and all of its worldwide subsidiaries which are owned or controlled, directly or indirectly, by Corning Incorporated. As used herein, ownership or control of an entity requires the direct or indirect ownership of stock or other interest representing more than fifty percent (50%) of the voting or other similar power for the election or appointment of directors, managers, general partners, or similar officials of such entity. This collective corporate family is sometimes also referred to herein as the "CORNING Group."

[2] "Personal Data" shall mean 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. 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.

[3] "Data transfer" shall mean any transfer of Personal Data from an entity to another entity. A transfer can be carried out via any communication, copy, transfer, or disclosure of Personal Data through a network, including remote access to a database or transfer from a medium to another, whatever the type of medium (for instance from a computer hard disk to a server).

data protection policies and procedures, employee training, and a program to periodically monitor compliance with data protection standards.

CORNING commits to making 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.

I. PURPOSE OF THE POLICY

The purpose of this Policy is:

i. to describe the standards that CORNING applies when it processes Personal Data
ii. to explain the governance actions implemented by CORNING as a group with regards to Personal Data protection.
iii. To outline the rights of the Data Subjects whose Personal Data is processed and how they can exercise those rights.

II. SCOPE OF THE POLICY

This Policy applies to the Processing[4] of all Personal Data carried out by or on behalf of any CORNING entity, irrespective of the format of such Personal Data (e.g., electronic records, paper files, video recordings, etc.).

CORNING entities, all CORNING employees, and contingent workers are required to comply with this Policy. In addition to the GDPR, each CORNING entity complies with applicable local data protection requirements.

In addition, all Suppliers[5] and, to the extent applicable, any Third Parties[6], entrusted with Personal Data by or on behalf of CORNING must provide satisfactory assurances of Personal Data protection standards that are at least equivalent to those contained in this Policy.

III. GENERAL RULE

CORNING is committed to protecting and safeguarding the Personal Data entrusted to it by its employees, applicants, contingent workers, customers, Suppliers, business partners, and others with whom it interacts, in accordance with the principles set forth in the BCRs and in this Policy.

CORNING's data protection practices and programs are aligned with CORNING's values and applicable laws and regulations. CORNING requires its Suppliers and

[4] "Processing" shall mean any operation performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
[5] "Supplier" shall mean a term used by Corning to refer to the majority of its Processors. A Supplier is an entity, under a contract, that may process personal data as directed by Corning, such as a payroll provider.
[6] "Third Party" shall mean a natural or legal person, public authority, agency or body, other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to process the data.

business partners to uphold data protection practices for the Personal Data entrusted to them which are at least as stringent as those detailed in CORNING's BCRs and in this Policy.

IV. DATA PROTECTION PRINCIPLES

Legal basis for processing Personal Data

CORNING collects and processes Personal Data only if:

- The Data Subject has given its Consent[7] to the Processing of his or her Personal Data for one or more specific purposes; or
- 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; or
- Processing is necessary for compliance with a legal obligation of CORNING; or
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person; or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in CORNING or in a Third Party to whom the Personal Data is disclosed; or
- Processing is necessary for the purposes of the legitimate interests pursued by CORNING acting as Controller[8] or by the Third Party or Parties to whom the Personal Data is disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the Data Subject which require protection in particular where the Data Subject is a child.

Legal basis for processing Special Categories of Personal Data[9]

CORNING does not process Special Categories of Personal Data unless:

- The Data Subject has unambiguously given his/her consent to the Processing of those Personal 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 Controller in the field of employment law in so far as it is authorized by Union or national law or a collective agreement 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 Consent; or
- The Processing Personal Data is necessary for the establishment, exercise or defense of legal claims; or
- The processing relates to Special Categories of Personal Data which is

[7] All capitalized terms not otherwise defined in this Policy have the meaning ascribed to them in the GDPR.
[8] "Controller" shall mean 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.
[9] "Special Categories of Personal Data" means personal data revealing data racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data, biometric data, data concerning health, data concerning a natural person's sex life or sexual orientation.

manifestly made public by the Data Subject; or
- The Processing is necessary for reasons of substantial public interest;
- The Processing is necessary for the assessment of the working capacity of the employee;
- The Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (in accordance with article 89 of the GDPR).

CORNING may process Personal Data relating to offenses, criminal convictions or security measures, in which case such processing of Personal Data shall only be carried out under the control of an official authority, where applicable, and in compliance with specific safeguards provided under applicable national law. In addition, local data protection laws may provide specific limitations for the Processing of national identification numbers.

Purpose limitation

CORNING processes Personal Data for specified, explicit, and legitimate purposes and does not further process it in a way that is incompatible with those purposes. CORNING does not process Personal Data for further purposes without verifying if either the prior Consent of the Data Subjects has been obtained; the Processing is based on a legal obligation; or the new Purpose of Processing is deemed compatible with the purpose for which the Personal Data was initially collected and processed.

Data quality and minimization

CORNING collects and processes 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.

CORNING limits the collection of Personal Data to what is appropriate and necessary for its business purposes. When processing Personal Data, CORNING ensures that it is adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed. The specific types of Personal Data that are collected for a particular purpose 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 information which was provided to the Data Subjects, CORNING shall, as appropriate, 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.

Accurate and 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. CORNING shall, as appropriate, take steps to ensure that Personal Data which is inaccurate or incomplete, in regard to the purposes for which it was collected or for which it is further processed, is erased or rectified. Data Subjects may contact the CORNING points 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.

Appropriate data retention

CORNING retains Personal Data consistent with legal and business retention requirements in a form which permits identification, and does not store Personal Data when it is no longer relevant for the purposes for which it has been collected and processed. In particular, CORNING takes reasonable steps to destroy the Personal Data when (i) it is no longer required for the purposes for which it was collected, and/or (ii) the maximum retention period allowed by applicable law (if any) has elapsed.

Automated individual decisions

CORNING takes appropriate steps to ensure that every Data Subject has the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated Processing of Personal Data, including profiling intended to evaluate certain personal aspects relating to him in the conditions provided by the applicable data protection rules (i.e., except if the decision is necessary for entering into, or performance of, a contract between the Data Subject and CORNING or is authorized by an applicable data protection law to which CORNING is subject or is based on the Data Subject's explicit consent).

Transparency and information right

In accordance with the principle of transparency, Corning ensures that information provided to Data Subjects is intelligible and accessible for Data Subjects. The information is presented in a concise, and easily accessible form, using clear and plain language.

CORNING provides Data Subjects with at least the following information, except where the Data Subject already has it:

- The identity and the contact details of the Controller and the Controller's representative, if any, and, when appropriate, the place in which the Controller is based outside the EEA;
- The contact details of the Data Protection Officer (appointed in compliance with the GDPR or other applicable EU data protection laws, where applicable);
- The purposes of the processing for which the Personal Data are intended, as well as the legal basis for the Processing;
- Where the Processing is based on legitimate interest, the legitimate interests pursued by the Controller or by a Third party
- The Recipients[10] or categories of Recipients of the Personal Data; where applicable, the transfer of Personal Data to a third country, and the details of the relevant safeguards, including the existence or absence of an adequacy decision by the European Commission, and the means by which to obtain a

[10] "Recipient" shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a Third Party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as Recipients.

copy of them or where they have been made available

- Any further information such as:
  - the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
  - whether the provision of Personal Data is statutory or contractual, whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;
  - the existence of automated individual decision making (if any), including profiling, including meaningful information about the logic involved, as well as the significance and the potential consequences of such Processing for the Data Subject;
  - The existence of the right to request from the Controller access to and correction or deletion of Personal Data or restriction of processing concerning the Data Subject or to object to Processing as well as the right to data portability of Personal Data;
  - Where the processing is based on consent the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
  - The right to lodge a complaint with a Supervisory Authority[11] in case of a breach to the data protection regulation.

In addition, according to Corning's commitments under the BCRs, in the information notice, Corning will also inform the Data Subjects that if the Data Subject suffers any damage related to the Processing of his or her Personal Data, the Data Subject is entitled, to obtain redress and, where appropriate, receive compensation as may be ordered by the competent court or Supervisory Authority or as decided according to the internal complaint mechanism, if used (see articles 5.4. 6.3. and 6.4 of the BCRs to know more about these specific rights.

Where the Personal Data has not been directly obtained from the Data Subjects, CORNING also provides the Data Subjects with the categories of Personal Data concerned and information with regard to the source from which the Personal Data originated, and if applicable, whether it came from publicly accessible sources. In such a case, the information above is provided:

a. within a reasonable period after obtaining the Personal Data, but at the latest within one month, having regard to the specific circumstances in which the Personal Data are processed;
b. if the Personal Data are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject; or
c. or if a disclosure to a Third Party is contemplated, no later than the time when the Personal Data are first disclosed.

The obligation to inform the Data Subjects does not apply if (i) the Data Subject

[11] "Supervisory Authority" shall mean means an independent body which is in charge of: (i) monitoring the Processing of Personal Data within its jurisdiction, (ii), providing advice to the competent bodies with regard to legislative and administrative measures relating to the Processing of Personal Data, and (iii) hearing complaints lodged by Data Subjects with regard to the protection of their data protection rights.

already has the information; or (ii) it would involve a disproportionate effort; or (iii) recording or disclosure of such Personal Data is expressly required by law to which the Controller is subject and which provides appropriate measures to protect the Data Subject's legitimate interests; or (iv) where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by EU or national law, including a statutory obligation of secrecy.

Right of access, correction, deletion, restriction of processing, right to object to the Processing and to data portability

CORNING implements adequate means to receive and respond to Data

Subject requests relating to their rights. Each Data Subject has the right to:

- Obtain from CORNING without constraint, at reasonable intervals, and without excessive delay or expense, and, where applicable, according to national legislation:
  - Confirmation as to whether or not Personal Data relating to the Data Subject is being processed,
  - If so, information at least as to the purposes of the processing, the categories of data concerned, and the Recipients or categories of Recipients to whom the Personal Data are disclosed; where possible the planned period for which the Personal Data will be stored or if not possible the criteria used to determine that period, the existence of the right to request from CORNING correction or deletion of Personal Data or restriction of Processing of Personal Data concerning the Data Subject or to object to such Processing, the right to lodge a complaint with a Supervisory Authority, any available information as to their source (where the Personal Data are not collected from the Data Subject); the existence of automated decision-making, including profiling and, at least, meaningful information about the logic involved, as well as the significance and the possible consequences of such Processing for the Data Subject;
  - Where Personal Data are transferred to a Third Country[12], information about the appropriate safeguards used for the Transfer; Communication to the Data Subject in an intelligible form of the Personal Data undergoing processing and of any available information as to their source;
- Obtain from CORNING without undue delay, the correction and deletion of inaccurate Personal Data concerning him or her, the deletion of Personal Data or restriction of Processing;
- Exercise his or her right to data portability and obtain from CORNING the right to receive the Personal Data concerning him or her, which he or she has provided to CORNING, in a structured, commonly used and machine-readable format;
- Object to, at any time on compelling legitimate grounds relating to the Data

[12] "**Third Country**" means a country located outside the European Economic Area (EEA).

Subject's particular situation, the processing of Personal Data (when the processing is based on the legitimate interest of CORNING);
- Object, at any time of the Processing and without having to state legitimate grounds, to the Processing of Personal Data for the purposes of direct marketing (including profiling to the extent that it is related to such direct marketing).

CORNING has a procedure in place to describe the roles and responsibilities related to providing Data Subjects with the rights to access, correct and delete Personal Data CORNING maintains about them, as well as the rights to object to the Processing of Personal Data, to obtain the restriction of the Processing or to obtain data portability.

Data Subjects may submit their requests to privacy@corning.com, at a local level to either the Appointed Data Protection Officer ("ADPO") or Local Privacy Contact ("LPC"), or other business function representative via postal mail, in person, via telephone or via email.

In order to enable CORNING to answer any request, the Data Subjects must communicate to CORNING the following necessary identification data: name, surname, e-mail or postal address and any other necessary information necessary to confirm their identity.

CORNING may object to requests that are obviously excessive, in particular by their number, or their repetitive and systematic character.

Right to lodge a complaint. Data Subjects also have the right to lodge a complaint with a Supervisory Authority if the Data Subject suspects that Corning is not compliant with applicable Personal Data protection regulations.

Security and confidentiality

CORNING has put in place appropriate and commercially reasonable technical and organizational security measures to keep Personal Data that it collects and holds confidential and to protect it against unauthorized or unlawful disclosure or access, accidental loss, destruction, alteration or damage, taking into consideration the state of art of technology and the cost of implementation. These measures are intended to ensure an appropriate level of security in relation to the risks inherent in 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 Suppliers who are given access to Personal Data uphold at least as stringent security measures as those applied by CORNING.

Personal Data Breach Notifications

Personal Data Breaches[13] are subject to a notification regime before competent

[13] "Personal Data Breach" shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data transmitted, stored or otherwise processed.

Supervisory Authorities and affected Data Subjects under certain circumstances.

CORNING ensures that adequate means are in place to respond to this obligation. In particular, CORNING employees shall report any suspected or actual Personal Data Breach (including loss of or damage to equipment containing Personal Data) to privacy@corning.com or the relevant ADPO or LPC. The Corning Privacy Office handles Personal Data Breaches with other relevant Corning stakeholders without undue delay.

Transfers of Personal Data within or outside the Corning Group

CORNING is a global organization, with legal entities around the world, and businesses, IT systems, management structures, and processes that cross borders. As such, it is often necessary for CORNING to transfer Personal Data to other CORNING entities, to Suppliers, 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. CORNING has adopted BCRs, a system of principles, rules and tools, provided by EU law, in an effort to ensure effective levels of data protection, in particular relating to Transfers of Personal Data to CORNING entities located outside the European Economic Area (EEA). More specifically:

- 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 the BCRs and with any stricter local laws applicable to the Transfer and to any subsequent processing (including onward transfer). As provided for in the BCRs, where a CORNING entity requests that another CORNING entity undertakes processing of Personal Data on its behalf, the CORNING entity receiving the processing services shall choose another CORNING entity providing sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out and must ensure compliance with those measures. Any CORNING entity which is bound by the BCRs undertakes to provide those sufficient guarantees and to comply with all safeguards contained in the BCRs when acting as a Processor[14] on behalf of another CORNING entity, in particular complying with the instructions provided by the CORNING entity transferring the personal data and implementing Technical and Organizational Security Measures to sufficiently protect the personal data against any accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access through a specific data processing agreement. In addition, if the Transfer takes place between two CORNING entities who act as Joint Controllers[15], a written agreement will be concluded stipulating their respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the exercising of the

[14] "Processor" shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the Controller.
[15] Two or more controllers who jointly determine the purposes and means of processing.

rights of the Data Subject.

- Transfers to entities outside of the CORNING Group:

- Suppliers: CORNING has entered or will enter into appropriate written contracts with Suppliers 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 Suppliers satisfactory assurances (i) of standards which are at least equivalent to those contained in this Policy (ii) and of compliance by the Supplier with applicable Data Protection Laws, in particular those applying to Personal Data Transfer and to any onward transfers. Such Suppliers will have access to Personal Data solely for the purposes of performing the services specified in their applicable service contracts. If a CORNING entity concludes that a Supplier is not complying with these obligations, it will promptly take appropriate actions. Furthermore, CORNING does not transfer Personal Data to Suppliers outside of the EU unless those suppliers have adopted appropriate privacy and security controls to protect personal data in accordance with the relevant EU data protection requirements (for instance by ensuring that the EU Standard Contractual Clauses approved by the EU Commission are signed with the Supplier if the latter is located in a country which does not provide an adequate level of protection of Personal Data). In addition, for Joint-Controllers relationship (if any), a written agreement will be concluded by Corning with any external Joint-Controllers in compliance with the GDPR.

- Third Parties: CORNING entities may be required to disclose certain Personal Data to 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).

Accountability

In order to demonstrate compliance with the principles set forth in this Policy, CORNING has implemented the following measures:

i) Records of Processing activities

CORNING maintains internal records of Processing activities involving Personal Data[16]. These records must be available to any competent Supervisory Authority for purposes of an investigation.

ii) Data protection by design and by default

CORNING must implement appropriate technical and organizational measures designed to implement Data Protection principles in an effective manner and integrate the necessary safeguards into the Processing in order to meet Data

[16] See Article 30 of the GDPR.

Protection requirements and protect the rights of the Data Subjects, both at the time of the determination of the means of Processing and at the time of Processing itself.

In addition, CORNING must implement appropriate technical and organizational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are processed. This rule applies to the amount of Personal Data collected, the period of their storage and their accessibility.

iii) Data protection impact assessments

CORNING carries out Data Protection Impact Assessments (or DPIAs) when processing is likely to result in a high risk to the rights and freedoms of Data subjects [17]. A DPIA assesses Processing activities to identify the impact that Processing might have on the rights and freedoms of Data Subjects and sets out recommendations for managing that impact.

V. COMMITMENT AND MEANS IMPLEMENTED TO COMPLY WITH THIS POLICY

CORNING has established the CORNING Privacy Office ("CPO"), made up of the Global Chief Privacy Officer ("GCPO"), Regional Data Privacy Managers, Appointed Data Protection Officers (where required according to the GDPR and/or applicable data protection law), and Local Privacy Contacts. The CPO is responsible at the CORNING Group level for compliance with this Policy and the BCRs and for initiating and coordinating any required evolution of this Policy and BCRs as well as related policies and procedures. CORNING also maintains programs to periodically monitor adherence to this Policy and to help ensure compliance of CORNING entities and employees with the BCRs, laws, requirements and contractual agreements that apply to the Personal Data processed.

Such programs include periodic training and audits that enable CORNING to verify that our Policy and our BCRs are accurate, comprehensive, prominently displayed, fully implemented, and accessible. Corning has implemented a training program to raise employee awareness of data protection issues. New employees and contingent workers who collect, process, or have access to Personal Data are required to complete a data protection training program. Furthermore, all employees who collect, process or have access to Personal Data shall be required to complete such a program, on a regular basis.

In addition, data protection compliance reviews will be carried out on a regular basis by internal or external teams to ensure that this Policy, the BCRs and all other related policies, procedures or guidelines are updated and applied.

VI. 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 or the

[17] Article 35 of the GDPR.

BCRs.

If a Data Subject believes that there has been a violation of the BCRs or of this Policy in that its Personal Data are processed in a way that is incompatible with the BCRs or this Policy, the Data Subject may lodge a complaint as described below.

CORNING has a procedure in place to describe the roles and responsibilities for handling data protection complaints received from Data Subjects and for receiving, documenting, investigating and responding to data protection complaints.

Corning.com has practical tools allowing Data Subjects to lodge their complaints, including at least one of the below:

- Web link to complaint form,
- Email address, Telephone number, or Postal address.

Data protection complaints submitted by employees

CORNING employees may submit data protection complaints through the Data Protection Complaint Form found on CORNING's intranet and on the external facing CORNING website. After completing the data protection complaint form, the form can be submitted via the following methods:

- Email to the CPO mailbox at privacy@corning.com
- Email, postal mail, or delivered in person to the Appointed Data Protection Officers or local Privacy Contacts or HR, Sales, Marketing, Global Supply Management, Finance, and Health and Safety departments as well as any other necessary business functions

Data protection complaints submitted by other Data Subjects (e.g., contingent workers, Suppliers, customers)

Other Data Subjects may submit data protection complaints through the data protection Complaint Form found on the external facing CORNING website. After completing the data protection complaint form, the form can be submitted via the following methods:

- Email, postal mail, or delivered in person to the Appointed Data Protection Officers or local Privacy Contacts, Customer Service representative, GSM representative or Sales and Marketing representative
- Email to the CPO mailbox at privacy@corning.com

When a complaint is registered, it is acknowledged and handled within a reasonable period of time (i.e. no later than one month of receipt of the request extended by two further months where necessary taking into account the complexity and number of requests). CORNING will inform the Data Subject of such extension if applicable.

If the Data Subject is not satisfied by the replies of the Corning, or if the Data Subject prefers to bypass the available internal complaint mechanism, the Data Subject has the right to lodge a complaint before the relevant Supervisory Authority[18] and/or seek recourse at the competent jurisdictions[19].

[18] Where the GDPR is applicable, in the EU Member State of the habitual residence of the Data Subject, of his place of work or place of the alleged infringement.
[19] Where the GDPR is applicable, the court of the Member State where the Local Data Controller has an

VII. CORNING POINTS OF CONTACT

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

Corning Privacy Office
One Riverfront Plaza
MP-HQ-01-E06
Corning, NY 14831
(607) 974-9000
Privacy@corning.com

If you are a CORNING employee, you may also contact your locations or Division's Appointed Data Protection Officer (if any) or Local Privacy Contact or HR designated contact.

VIII. AMENDMENTS

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

establishment or where the Data Subject has his habitual residence.