Alcon Global Policy on the Protection of Personal Data

1. PURPOSE

This purpose of this policy is to establish minimum global requirements for the fair and lawful collection, processing, handling, and protection of Personal Data by and on behalf of Alcon, consistent with Alcon's commitment to the protection of Personal Data. Protecting this information is crucial to preserving the Data Subjects' trust in Alcon, as well as Alcon's brand and reputation.

2. SCOPE

This policy applies globally to all Alcon associates and affiliates that collect, have access to, and/or Process Personal Data, whether the Personal Data belongs to consumers, patients, healthcare professionals, other Alcon customers and business partners, or associates.

This policy supersedes any less strict local requirements. Local privacy-related laws or regulations that are more strict than this policy must be followed. Associates are encouraged to consult with the Alcon Global Privacy Office or their local legal support teams where local privacy regulations are in force.

3. POLICY

3.1 General Requirements

3.1.1 *Purpose and Manner* – Alcon may collect and Process Personal Data only when:

- There is a legitimate business purpose for collecting the Personal Data that is acceptable under the local law where the information is collected, and
- The information is collected and Processed in an appropriate manner, consistent with local legal requirements.

3.1.2 *Principles* – The following principles apply to Alcon's collection of Personal Data:

- **Principle of transparency** – The collection and purpose of the Processing must be evident to the Data Subject.
- **Principle of proportionality / data minimization** – Only Personal Data that is relevant to the stated purpose may be collected.
- **Principle of purpose limitation** – Personal Data may only be Processed for the purpose that is (i) indicated at the time of collection, (ii) evident from the circumstances, or (iii) provided for by law.

3.2 Notice – For any Process that collects Personal Data from individuals, a privacy notice must be provided to the Data Subjects at the point where the Personal Data is first collected. The notice must provide information about why and how their Personal Data will be Processed by Alcon.

The notice can be communicated to the Data Subject in multiple ways, including electronically or via printed materials. Regardless of the form it takes, the information provided must be written in clear language. If the point of collection is online, a link to the

notice must be provided on the same web page where the Personal Data collection takes place.

3.3 Consent – Consent of the Data Subject may be required prior to processing certain types of Personal Data, including Sensitive Personal Data.

If consent is required, the consent must be freely given, explicit, specific, informed, and unambiguous. Consent is freely given if a real choice is offered to the Data Subject and there is no inappropriate pressure or influence that could affect the Data Subject's choice.

3.4 Sensitive Personal Data – Sensitive Personal Data requires a higher standard of protection and safeguards. Safeguards may be physical, such as locks and access cards for buildings, electronic, such as encryption and passwords, or organizational, such as restricting access to information to only those who need it.

Sensitive Personal Data must not be disclosed to third parties without an appropriate legal basis. In many cases, the Data Subject must provide informed, voluntary, and explicitly consent to the disclosure.

3.5 Data Lifecycle Management

3.5.1 *Privacy by design* – Alcon is committed to protecting Personal Data through privacy by design, by implementing technological controls and administrative safeguards, into the fundamental design of systems, products, and marketing programs.

3.5.2 *Electronic Privacy Assessments and Data Protection Impact Assessments* – Whenever a business process owner proposes to begin Processing new types of Personal Data, or makes changes to existing Processing of Personal Data, the business process owner must collaborate with the Global Privacy Office to evaluate the changes using Alcon privacy tools and templates such as the Electronic Privacy Assessment (ePA) tool or the Data Protection Impact Assessment (DPIA) tool.

For additional details regarding the ePA or DPIA tools, please refer to the Privacy Policy Reference Table or contact the Global Privacy Office.

3.5.3 *Inventory* – Where required by local law, Alcon will maintain an inventory of relevant Processing activities.

For more information regarding Alcon's inventory practices, please refer to the Privacy Policy Reference Table.

3.6 Retention of Personal Data – Alcon may retain Personal Data in an identifiable form only for as long as the data is required for the purposes for which Alcon collected it. Associates must comply with the applicable data retention periods established by Alcon. Personal Data that is no longer needed for the original purpose must be destroyed or anonymized.

For additional details about Alcon's data retention guidelines, please refer to the Privacy Policy Reference Table.

3.7 Data Security

3.7.1 *Safeguards* – Alcon has reasonable administrative, technical, and physical security safeguards in place to protect Personal Data Processed by Alcon against loss, theft, misuse, and unauthorized access, modification, disclosure, copying, or other Processing.

For additional details regarding Alcon's Data Security practices, see the Privacy Policy Reference Table.

3.7.2 *Data security incidents* – Any misuse, loss, or unauthorized access, modification, or disclosure of Personal Data is called a data security incident.

If a data security incident involves the loss of or unauthorized access to Personal Data, local law may require that a notification of a data breach be given to the local data protection regulatory authority or to the affected Data Subjects. Associates must immediately report any suspected and actual data security incidents to the Alcon Ethics Hotline or the Global Privacy Office for further evaluation.

For more guidance regarding handling Data Security Incidents, refer to the Privacy Policy Reference Table.

3.8 Engaging Third Party Data Processors – Alcon requires that suppliers, vendors, or other third parties that collect, use, disclose, store, or otherwise Process Personal Data on behalf of Alcon have appropriate data protection safeguards in place.

Before contracting with a third party to Process Personal Data:

- Associates must follow the company vetting Process for evaluating the third party's data protection capabilities.
- A written agreement with appropriate contractual terms for handling Personal Data must be signed before the Personal Data is Processed by the third party.

Refer to the materials listed in the Privacy Policy Reference Table for additional information.

3.9 Data Subject Rights Requests – To the extent it is feasible to do so, Alcon will permit Data Subjects to review the Personal Data that Alcon holds about them, and to allow Data Subjects to correct or amend Personal Data in cases where it may be incomplete or inaccurate.

Some local laws provide additional rights to Data Subjects, including the rights to erase data or transport the data in an electronic format. Requests by any individual to review, edit, change, delete, or transport their Personal Data are called Data Subject Rights (DSR) Requests. Associates must immediately direct DSR Requests to the Alcon Global Privacy Office for further follow-up.

For additional information regarding DSR requests, refer to the Privacy Policy Reference Table.

4. GLOSSARY

Data Subject	A natural living person whose Personal Data is Processed by or on behalf of Alcon (such as an Alcon customer or associate).
Personal Data	Any information relating to an identified or identifiable individual. An identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or one or more factors specific to his identity. Examples of Personal Data include name, address, location data, email address (including business email address), or credit card number. Other examples of Personal Data may include online identifiers, IP addresses, browsing history, or purchasing history.
Process	Any operation performed on Personal Data (regardless of whether it is automated or manual). Examples of Processing include the collection of data; archiving data for public interest, scientific or historical research, or statistical purposes; or otherwise storing, organizing, adapting or altering, combining, retrieving, consulting, using, disclosing, transmitting, disseminating, blocking, erasing, or destroying Personal Data.
Sensitive Personal Data	Personal Data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their Processing could create significant risks to the fundamental rights and freedoms. Examples of Sensitive Personal Data include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, social security or insurance information, criminal charges, conviction / sentence, or a person's sexual orientation, or health information. Data elements that make up Sensitive Personal Data may vary by country and local law should be consulted.