

NOTICE ON THE PROCESSING OF CUSTOMERS AND SUPPLIERS PERSONAL DATA and PRIVACY POLICY

In connection with the processing of customers and suppliers personal data (specifically of the contact persons), the following information is provided.

1. Data Controller

The Data Controller is **Marcolin U.S.A. Eyewear Corp** with registered office in 3140 Route 22 West, Somerville, New Jersey 08876, USA (hereinafter referred to as the “Company” or the “Data Controller”).

This Privacy Policy describes how (“Marcolin”) handles the personal information of individuals to whom we market and provide our services, of individuals who provide us their services, as well as the information we collect on our website, from third parties, and from other sources.

We treat all personal information covered by this Privacy Policy, including information about any visitors to our website, as pertaining to individuals acting as business representatives, and not in their individual or household capacity.

2. Type of Data Processed, Purpose and Legal Basis of the Processing

The following data are collected and processed by the Data Controller:

- Common personal data (contact data, first name, surname, function, e-mail) of the customer or supplier for pre-contractual and contractual performance purposes, and for administrative-accounting-fiscal obligations connected with invoicing. Therefore, the legal basis for the data processing is the performance of contractual and legal obligations.
- Common personal data such as contact data, first name, surname, function, e-mail of the customer/customer personnel, subject to consent, for the purpose of sending marketing communications (i.e. newsletter communications, invitations to events). The legal basis for the data processing is the consent.
- Common personal data such as contact data, first name, surname, function, e-mail of the customer/customer personnel for the purpose of sending commercial communications for products or services that are identical or similar to the products/services subject to the contract with the customer (soft spam), survey and update of company services to the customer, unless the customer objects. The legal basis for the data processing is the Data Controller’s legitimate interest in improving the contractual and customer satisfaction service.
- Common personal data (contact data, first name, surname, function, e-mail) processed for organisational, administrative and accounting purposes, based on the Data Controller’s legitimate interest in the optimisation and coordination of processes and services.
- the Customer’s personal data (such as first name, surname, e-mail and telephone number) may be processed for the purpose of providing the Multi-Factor Authentication (MFA) service for access to the *mymarcolin* website, for security purposes, by blocking unauthorised access to the Customer’s personal account. The legal basis for the processing is the consent given by the Customer to the activation of the MFA service.

3. Disclosure of Data to Third Parties - Transfer outside the EU

The Company may transfer the data processed for the abovementioned purposes to: (i) internal company parties in charge of processing; (ii) external parties belonging to the following categories: external consultants, service companies (transport, shipping, marketing and IT services companies, tax and credit services companies), the company’s sales network (agents), banking institutions, supervisory bodies; (iii) other companies of the

Marcolin/Vision Service Plan Group, also established in the United States. Data shall be transferred in the United States to other Group companies (Vision Service Plan is headquartered in California) in accordance with the GDPR and based on appropriate safeguards, such as the adoption of the standard data-protection clauses adopted by the European Commission.

4. Processing Methods, Data Retention Period and Criteria

The data will be processed in hard copy and digital format, and will be kept for the period necessary to fulfil the abovementioned purpose(s), and specifically, respectively:

- (i) for the statutory limitation period relating to the retention of contracts and administrative data and/or for the defence of legal claims, where necessary (ten years from the last use and/or limitation interruption event);
- (ii) due to the data subject's dissent/opt-out, i.e. until they unsubscribe from marketing communications and up to a maximum of two (2) years from the last consent given or the last expression of interest;
- (iii) , (iv), (v) for the duration of the contractual relationship and in any case up to a maximum of two (2) years from the last expression of interest.

5. Data Provision

The provision of the data referred to in point 2 shall be considered:

- (iv) mandatory for the performance of the contractual relationship and for legal purposes. Failure to provide data will make it impossible to pursue the above-mentioned purposes.
- (v) optional for marketing communications, to the extent that the data subject may at any time object to the processing by expressing dissent/opting-out in the dedicated section "Manage Preferences or Unsubscribe", to be found at the bottom of each communication.
- (vi) optional for surveys and for the updating of company services and soft spam communications to the customer, as the customer may object to the processing by expressing dissent/opting-out in the dedicated section "Manage Preferences | Unsubscribe", to be found at the bottom of each communication.

6. Rights of the Data Subject, Withdrawal of Consent and Complaint to the Supervisory Authority

The data subject has the right, at any time, to request access to, rectification, erasure, restriction of their personal data, to object to processing and to exercise the right to data portability.

In any case, the data subject has the right, at any time, to withdraw the consent given to the processing of data, without prejudice to the lawfulness of the processing based on the consent given before the withdrawal.

In the event of an alleged breach, data subjects, if the conditions are met, also has the right to lodge a complaint with a Data Protection Supervisory Authority located in the State where they usually reside, or in the State where they work or where the alleged breach took place.

7. Profiling and Automated Decision-Making Processes

Processing is not carried out by means of automated decision-making processes (e.g. profiling).

Marcolin USA Privacy Policy

This Privacy Policy describes how Marcolin U.S.A. Eyewear Corp (“Marcolin”) handles the personal information of individuals to whom we market and provide our services, of individuals who provide us their services, as well as the information we collect on our website, from third parties, and from other sources.

We treat all personal information covered by this Privacy Policy, including information about any visitors to our website, as pertaining to individuals acting as business representatives, and not in their individual or household capacity.

1. Personal Information We Collect

- Business contact details, such as your first and last name, business e-mail address, business mailing address, and I-9 information such as driver’s license, social security number, and passport number.
- Payment and transaction data needed to complete your orders on or through the services (including name, payment card information, bank account number, billing information), and your purchase history. This information is processed directly by our third party payment service provider.
- Communications that we exchange with you, including when you contact us with questions, feedback, or otherwise.
- Other data not specifically listed here, which we will use as described in this Privacy Policy or as otherwise disclosed at the time of collection.

2. Third party sources

We may combine personal information we receive from you with personal information we obtain from other sources, such as:

- Third parties, such as data providers, event co-sponsors, and others.
- Public sources, such as social media platforms.

3. Automatic data collection

We, and our service providers, may automatically log information about you, your computer or mobile device, and your interaction over time with our website and services

(in your capacity as our customer’s authorized user), our communications and other online services, such as:

- Device data, such as your computer’s or mobile device’s operating system type and version, manufacturer and model, browser type, screen resolution, RAM and disk size, CPU usage, device type (e.g., phone, tablet), IP address, unique identifiers (including identifiers used for advertising purposes), language settings, mobile device carrier, radio/network information (e.g., WiFi, LTE, 3G), and general location information such as city, state or geographic area.
- Online activity data, such as pages or screens you viewed, how long you spent on a page or screen, the website you visited before browsing to the website, navigation paths between pages or screens, information about your activity on a page or screen, access times, and duration of access, and whether you have opened our marketing emails or clicked links within them.
- Cookies, which are text files that websites store on a visitor’s device to uniquely identify the visitor’s browser or to store information or settings in the browser for the purpose of helping you navigate between pages efficiently, remembering your preferences, enabling functionality, helping us understand user activity and patterns, and facilitating online advertising.
- Local storage technologies, like HTML5, that provide cookie-equivalent functionality but can store larger amounts of data, including on your device outside of your browser in connection with specific applications.
- Web beacons, also known as pixel tags or clear GIFs, which are used to demonstrate that a webpage or email was accessed or opened, or that certain content was viewed or clicked.

4. How we use personal information

- Service delivery.

We use your personal information to:

- Provide, operate and improve our services and our business;
- Communicate with you about the services, including by sending announcements, updates, security alerts, and support and administrative messages; and
- Provide support for our services, and respond to your requests, questions and feedback.

- Research and development.

As part of these activities, we may create aggregated, de-identified or other anonymous data from personal information we collect. We may use this anonymous data and share it with third parties for our lawful business purposes, including to analyze and improve our services, and promote our business.

- Direct marketing.

We may send you direct marketing communications as permitted by law, including, but not limited to, notifying you of special promotions, offers and events via postal mail, email, telephone, text message, and other means. You may opt out of our marketing communications as described in the [“Opt out of marketing communications”](#) section below.

- Compliance and protection.

We may use your personal information to:

- Comply with applicable laws, lawful requests, and legal process, such as to respond to subpoenas or requests from government authorities;
- Protect our, your or others’ rights, privacy, safety or property (including by making and defending legal claims);
- Audit our internal processes for compliance with legal and contractual requirements and internal policies;
- Enforce the terms and conditions that govern our website and services; and
- Prevent, identify, investigate and deter fraudulent, harmful, unauthorized, unethical or illegal activity, including cyberattacks and identity theft.

5. How We Share Personal Information

We may share your personal information with:

Affiliates. Our corporate parent, subsidiaries, and affiliates, for purposes consistent with this Privacy Policy.

Service providers. Companies and individuals that provide services on our behalf or help us operate our services or our business (such as hosting, information technology, customer support, e-mail delivery, payment processing and website analytics services).

Professional advisors. Professional advisors, such as lawyers, auditors, bankers and insurers, where necessary in the course of the professional services that they render to us.

Authorities and others. Law enforcement, government authorities, and private parties, as we believe in good faith to be necessary or appropriate for the compliance and protection purposes described above.

Business transferees. Acquirers and other relevant participants in business transactions (or negotiations for such transactions) involving a corporate divestiture, merger, consolidation, acquisition, reorganization, sale or other disposition of all or any portion of the business or assets of, or equity interests in, Marcolin or our affiliates (including, in connection with a bankruptcy or similar proceedings).

6. Your Choices

Opt out of marketing communications. You may opt out of marketing-related communications by following the opt out or unsubscribe instructions contained in the marketing communications we send you.

Online tracking opt-out. There are a number of ways to limit online tracking, which we have summarized below:

- **Blocking cookies in your browser.** Most browsers let you remove or reject third party cookies. To do this, follow the instructions in your browser settings. Many browsers accept cookies by default until you change

your settings. For more information about cookies, including how to see what cookies have been set on your device and how to manage and delete them, visit www.allaboutcookies.org.

- Using privacy plug-ins or browsers. You can block our websites from setting cookies by using a browser with privacy features, like [Brave](#), or installing browser plugins like [Privacy Badger](#), [Ghostery](#), or [uBlock Origin](#), and configuring them to block third party cookies/trackers. You can also opt out of Google Analytics by downloading and installing the browser plug-in available at: <https://tools.google.com/dlpage/gaoptout>.

Note that because these opt out mechanisms are specific to the device or browser on which they are exercised, you will need to opt out on every browser and device that you use.

Do Not Track. Some Internet browsers may be configured to send "Do Not Track" signals to the online services that you visit. We currently do not respond to "Do Not Track" or similar signals. To find out more about "Do Not Track," please visit <http://www.allaboutdnt.com>.

7. Other Sites and Services

Our services may contain links to websites and other online services operated by third parties. These links and integrations are not an endorsement of, or representation that we are affiliated with, any third party. In addition, our content may be integrated into web pages or other online services that are not associated with us. We do not control websites or online services operated by third parties, and we are not responsible for their actions.

8. Security

We employ a number of technical, organizational and physical safeguards designed to protect the personal information we collect. However, no security measures are failsafe and we cannot guarantee the security of your personal information.

9. Children

Our services are not intended for use by children under 13 years of age. If we learn that we have collected personal information through our services from a child under 13 without the consent of the child's parent or guardian as required by law, we will delete it.

10. Changes to This Privacy Policy

We reserve the right to modify this Privacy Policy at any time. If we make material changes to this Privacy Policy, we will notify you by updating the date of this Privacy Policy and posting it on the website.

11. How to Contact Us

To find out the list of appointed Privacy Representatives and data processors, to obtain more information about the transfer of data to non-EU countries (including the USA) and the safeguards adopted to protect your data, to withdraw the consent given or to exercise your rights, you may send a request to the following e-mail address: infousa@marcolin.com