PERSONAL DATA PROTECTION POLICY

Compliance with GDPR (EU 2016/679), CCPA/CPRA (California),
Law 1581 of 2012 (Colombia) and LFPDPPP (Mexico)

Data Controller Details

Company Name	Julius Connected 2 Grow, S.A.P.I. de C.V. (and its subsidiaries in the U.S. and Colombia)
Website	www.julius2grow.com
Last Updated	June 2026
Version	1.0

Entities and Offices

Mexico (Headquarters)

Address	Benito Juarez 1102, Floor 5 South - Suite A, Monterrey Centro, Monterrey, Nuevo Leon, ZIP 64000, Mexico
Phone	+52 81 8335 1500
Email	mexico@julius2grow.com
DPO / Privacy Contact	privacidad@julius2grow.com

United States

Address	SW 8th St PMB 699, Miami, Florida 33130, U.S.A.
Email	usa@julius2grow.com
DPO / Privacy Contact	privacy@julius2grow.com

Colombia

Address (Bogota)	Carrera 7 # 84A - 29, Cabrera Building Of. 703, Bogota, Cundinamarca 110221, Colombia
Address (Medellin)	Calle 19 # 27 - 323, Via Las Palmas, Medellin, Antioquia 050021, Colombia
Email	colombia@julius2grow.com

DPO / Privacy Contact	datos@julius2grow.com

1. Introduction and Purpose

Julius Connected 2 Grow (hereinafter "JULIUS" or "the Company") is a digital marketing and business growth agency formed by the merger of Arkix and MKX, with offices in Mexico, the United States, and Colombia, providing services in e-commerce, digital content, digital strategy, performance marketing, marketing automation, and technology.

This Personal Data Protection Policy (hereinafter "the Policy") establishes the principles, obligations, and procedures that JULIUS applies to ensure the lawful, fair, and transparent processing of personal data belonging to its clients, prospects, employees, suppliers, and visitors to the website www.julius2grow.com.

This Policy complies with the requirements of the General Data Protection Regulation of the European Union (GDPR - Regulation EU 2016/679), the California Consumer Privacy Act (CCPA) and its amendment the California Privacy Rights Act (CPRA), Law 1581 of 2012 of Colombia and its Regulatory Decree 1377 of 2013, and the Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP) of Mexico.

2. Personal Data We Collect

2.1 Data collected directly

JULIUS collects the following personal data through contact forms, job application forms, and other communication channels on the website:

- Full name
- Email address
- Phone number
- Company name and job title
- Country and city of residence
- Message or specific inquiry
- Resume/CV information (for job applications)

2.2 Automatically collected data

When you visit www.julius2grow.com, technical and behavioral data is automatically collected through cookies and similar technologies:

- IP address and approximate geolocation data
- Device type, operating system, and browser
- Pages visited, time spent, and clicks
- Traffic source and search keywords
- Analytical and advertising cookie identifiers

2.3 Data from third parties and partners

JULIUS may receive personal data from social media platforms (Meta, LinkedIn, Google), CRM tools, and web analytics partners, where the data subject has given consent on those platforms in accordance with their own privacy policies.

3. Purposes of Processing

3.1 Primary purposes

- To respond to requests for information, quotes, or service demonstrations.
- To manage talent recruitment and hiring processes.
- To provide the services contracted by clients.
- To manage commercial and administrative relationships with clients and suppliers.
- To comply with legal, tax, and accounting obligations.

3.2 Secondary purposes (require consent)

- Sending commercial communications, newsletters, and service updates.
- Analysis of user behavior to improve the digital experience.
- Profiling for segmented marketing campaigns.
- Sharing information with business partners for co-marketing activities.

The data subject may at any time withdraw their consent for secondary purposes without affecting the lawfulness of prior processing.

4. Legal Basis for Processing

JULIUS bases the processing of personal data on the following legal grounds, applicable according to the regulations of each jurisdiction:

Legal Basis	Description	Applicable Regulation
Consent	The data subject has given explicit consent for processing.	GDPR Art. 6(1)(a) | CCPA SS 1798.100 | Law 1581 Art. 9 | LFPDPPP Art. 8
Contract performance	Processing is necessary to execute a contract with the data subject.	GDPR Art. 6(1)(b) | LFPDPPP Art. 16
Legal obligation	Processing is necessary to comply with legal obligations.	GDPR Art. 6(1)(c) | LFPDPPP Art. 10
Legitimate interest	Statistical analysis, IT security, and service improvement.	GDPR Art. 6(1)(f)

5. Data Subject Rights

5.1 Rights under GDPR (Data subjects in the European Union)

- Right of access (Art. 15): to know what data JULIUS processes and for what purposes.
- Right to rectification (Art. 16): to correct inaccurate or incomplete data.
- Right to erasure or right to be forgotten (Art. 17): to request deletion of your data.
- Right to restriction of processing (Art. 18).
- Right to data portability (Art. 20): to receive your data in a structured format.
- Right to object (Art. 21): to object to processing based on legitimate interest.
- Right not to be subject to automated decision-making (Art. 22).

5.2 Rights under CCPA/CPRA (California residents)

- Right to know what personal information is collected, used, disclosed, and sold.

- Right to delete personal information collected.
- Right to non-discrimination for exercising your rights.
- Right to opt out of the sale or sharing of personal information ("Do Not Sell or Share").
- Right to limit the use of sensitive personal information.
- Right to correct inaccurate personal information.

California residents may exercise these rights by contacting: privacy@julius2grow.com or by sending a request to: SW 8th St PMB 699, Miami, Florida 33130, U.S.A.

5.3 Rights under Law 1581 of 2012 (Data subjects in Colombia)

- To know, update, and rectify personal data.
- To request proof of the authorization granted.
- To be informed about the use given to personal data.
- To file complaints with the Superintendence of Industry and Commerce (SIC).
- To revoke authorization and/or request deletion of data.
- To access personal data free of charge.

5.4 Rights under LFPDPPP (Data subjects in Mexico) - ARCO Rights

- Access: to know the personal data held in our databases.
- Rectification: to correct data that is inaccurate or incomplete.
- Cancellation: to request that personal data be deleted.
- Opposition: to object to the processing of data for specific purposes.

To exercise ARCO rights in Mexico, contact: mexico@julius2grow.com | +52 81 8335 1500.

6. Procedure for Exercising Rights

To exercise any of the rights described in this Policy, the data subject must submit a request containing:

- Full name and valid official identification (copy or document number).
- Clear description of the right to be exercised and the data involved.
- Email address or postal address to receive a response.
- Documentation proving legal representation (if applicable).

JULIUS will acknowledge receipt of the request within no more than 5 business days and will respond within the following timeframes:

GDPR (EU)	Response within 30 calendar days (extendable by 60 additional days in complex cases).
CCPA/CPRA (California)	Response within 45 calendar days (extendable by 45 additional days).
Law 1581 (Colombia)	Inquiries: 10 business days. Claims: 15 business days (extendable by 8 days).
LFPDPPP (Mexico)	Response within 20 business days (extendable by 20 additional business days).

7. Data Transfers and Disclosure

7.1 Internal recipients

Personal data may be shared between Julius Group entities (Mexico, U.S., and Colombia) for the purposes described in this Policy, under confidentiality and internal transfer agreements that guarantee the same level of protection.

7.2 Service providers (Data Processors)

JULIUS may engage technology providers, cloud platforms, analytics tools, and CRM systems as data processors, who may only process data in accordance with documented instructions from JULIUS and under contracts that guarantee adequate security measures (DPAs under GDPR; standard contractual clauses or equivalent).

7.3 International transfers

When data is transferred outside the European Economic Area, JULIUS ensures appropriate safeguards through: Standard Contractual Clauses approved by the European Commission; adequacy decisions; or Binding Corporate Rules (BCR), as applicable.

For transfers from Colombia, the authorization procedure set out in Decree 1377 of 2013 will be followed.

7.4 Disclosure to third parties

JULIUS does not sell personal data to third parties. Data may only be disclosed in the following circumstances:

- Competent authorities when required by law or court order.
- Business partners or co-sponsors of events, with prior express authorization from the data subject.
- In the event of a merger, acquisition, or corporate restructuring, with prior notification.

8. Cookie Policy and Similar Technologies

The website www.julius2grow.com uses cookies and similar technologies to personalize content and advertisements, provide social media features, and analyze traffic. We also share information about your use of the website with our social media, advertising, and web analytics partners.

Cookie Type	Purpose	Legal Basis
Strictly Necessary	Essential website operation, authentication, and security.	Legitimate interest / Contractual necessity
Analytics	Google Analytics: traffic analysis, behavior, and performance metrics.	Consent
Advertising & Remarketing	Meta Pixel, Google Ads: campaign targeting and measurement.	Consent
Functional	Language, region, and user configuration preferences.	Consent

Users can manage their cookie preferences through the settings panel available on the website or through their browser settings. Disabling strictly necessary cookies may affect the functioning of the website.

9. Security Measures

JULIUS implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing, including:

- Data encryption in transit (TLS/SSL) and at rest (AES-256).
- Role-based access control (RBAC) and multi-factor authentication (MFA).
- Password management policies and secure sessions.
- Regular security audits and penetration testing.
- Incident response plans and security breach management.
- Staff training and awareness on data protection matters.
- Confidentiality agreements with all employees and suppliers.

10. Security Breach Notification

In the event of a security breach affecting personal data, JULIUS will follow the procedures established by each applicable regulation:

- GDPR: notification to the competent supervisory authority within 72 hours; notification to affected data subjects where there is a high risk.
- CCPA/CPRA: notification to affected individuals without unreasonable delay; report to the California Attorney General where applicable.
- LFPDPPP (Mexico): notification to the INAI and affected data subjects as promptly as possible.
- Law 1581 (Colombia): notification to the SIC and implementation of corrective measures.

11. Data Retention Periods

Personal data will be retained only for as long as is strictly necessary to fulfill the purposes for which it was collected and to comply with the corresponding legal obligations:

Contact data / prospects	3 years from last contact or until consent is withdrawn.
Client data	Duration of contract + 5 years (tax and legal obligations).
Unsuccessful job applicants	1 year from the end of the recruitment process.
Employee data	Duration of employment + 5 years (labor obligations).
Analytics cookie data	13 months from the user's last activity.
Advertising cookie data	As configured by each platform (max. 24 months).

12. Data of Minors

JULIUS services and website are not directed at persons under the age of 16 (or the equivalent minimum age under applicable local law). JULIUS does not knowingly collect personal data from minors. If it is discovered that data has been collected from a minor without adequate parental consent, such data will be deleted immediately.

13. Policy Updates

JULIUS reserves the right to modify this Policy at any time to reflect regulatory changes, new processing purposes, or operational updates. Modifications will be published at www.julius2grow.com with an indication of the effective date.

When changes are substantial, JULIUS will notify data subjects whose data is being processed through the usual communication channels (email or prominent notice on the website), with a minimum of 30 days advance notice before the changes take effect.

14. Supervisory Authorities

Data subjects who consider that the processing of their data does not comply with applicable regulations have the right to lodge a complaint with the competent supervisory authority:

European Union (GDPR)	Data Protection Authority of the relevant Member State (e.g., ICO in the UK, AEPD in Spain, CNIL in France).
Spain	Agencia Espanola de Proteccion de Datos (AEPD) - www.aepd.es
Mexico (LFPDPPP)	Instituto Nacional de Transparencia, Acceso a la Informacion y Proteccion de Datos Personales (INAI) - www.inai.org.mx
Colombia (Law 1581)	Superintendencia de Industria y Comercio (SIC) - www.sic.gov.co
California (CCPA/CPRA)	California Privacy Protection Agency (CPPA) - cppa.ca.gov

15. Data Protection Officer (DPO)

JULIUS has appointed a Data Protection Officer (DPO) responsible for overseeing compliance with this Policy and acting as a point of contact for data subjects and supervisory authorities. The DPO can be reached through the following channels:

DPO Mexico	privacidad@julius2grow.com | Benito Juarez 1102, Floor 5 South - Suite A, Monterrey, N.L. 64000, Mexico
DPO United States	privacy@julius2grow.com | SW 8th St PMB 699, Miami, Florida 33130, U.S.A.
DPO Colombia	datos@julius2grow.com | Carrera 7 # 84A - 29 Of. 703, Bogota / Calle 19 # 27 - 323, Medellin
Website	www.julius2grow.com