

PRIVACY POLICY – Ctrl365 S.A.

Last updated: January 2026

1. Who we are

We are **Ctrl365 S.A.** (“**Ctrl365**”, the “**Company**” or “**we**”), a company dedicated to the implementation of technology and automation solutions. We respect your privacy and are committed to protecting your personal data.

In this Policy we describe what information we may collect or that you may provide when you:

- visit our website <https://ctrl365.com> (the “**Website**”),
- complete forms on our landing pages,
- download material (such as case studies),
- register for events, webinars or masterclasses,
- or interact with our commercial and marketing communications.

We also explain our practices for collecting, using, storing, protecting and, where applicable, sharing that information.

Data Controller

The primary controller of the personal data collected through the Website and our associated tools is:

Ctrl365 S.A. – CUIT 30-71412704-3
Registered address: Av. Leandro N. Alem 734, 5th Floor, C.A.B.A. (1001), Buenos Aires, Argentina

Contact email for privacy and data subject rights: legales@ctrl365.com

Ctrl365 S.A. centrally manages the Website, forms, CRM, analytics, marketing campaigns and the operational processes associated with the processing of personal data.

Joint Controllers

The following companies act as **joint controllers**, as they are operationally involved in the commercial, administrative and service-related management connected to the data collected through the Website. They share infrastructure, teams, processes and systems:

- **Instalnet S.R.L.**
CUIT 30-71016130-1
Registered address: Av. Leandro N. Alem 734, 5th Floor, C.A.B.A. (1001), Buenos Aires, Argentina
- **RPA365 S.A.**
CUIT 30-71652626-3
Registered address: Av. Leandro N. Alem 734, 5th Floor, C.A.B.A. (1001), Buenos Aires, Argentina
- **Arkademy S.A.**
CUIT 30-71657882-4
Registered address: Av. Leandro N. Alem 734, 5th Floor, C.A.B.A. (1001), Buenos Aires, Argentina

These companies participate in the integrated operational activity of Ctrl365 and may access, use or manage personal data in accordance with the same internal policies, security measures and purposes described in this Privacy Policy.

All requests to exercise data subject rights (access, rectification, update, deletion, objection, etc.) will be handled centrally by Ctrl365 S.A. on behalf of all joint controllers.

By accessing or using the Website or our forms, you agree to this Privacy Policy. This Policy may be updated; continued use after any change implies acceptance of the current version. We recommend reviewing it periodically.

2. Scope of this Policy

This Privacy Policy applies to:

- the Website <https://ctrl365.com> and its sections,
- campaign- and solution-specific landing pages,
- contact forms, content-download forms, event and webinar registration forms,
- marketing processes and commercial contact activities managed by Ctrl365.
-

In some cases, specific campaigns or actions may include additional privacy terms, which will complement this Policy. Some campaigns may use landing pages hosted on HubSpot CMS. In those cases, this Policy applies and is complemented by the provider's policies.

3. Personal data we collect

We collect different categories of personal data depending on how you interact with Ctrl365:

a) Data you provide directly

When you complete forms on the Website or our landing pages, or when you contact us through enabled channels, we may request:

- First and last name
- Email address (corporate)
- Telephone number
- Company
- Job title or role
- Country
- Area of interest (for example: RPA, Copilot, Cybersecurity, Licensing, Artificial Intelligence, Discovery, etc.)
- Reason for your inquiry or any other free-text information you decide to share

We may also collect information when you register for events, webinars or masterclasses, or when you download resources such as case studies. If you voluntarily choose to send us your **curriculum vitae (CV)** to the email address indicated on our Website (recruiting@ctrl365.com), we will also process the information contained in your CV.

b) Data collected automatically

When you browse our Website, we may automatically collect certain information through cookies and similar technologies, such as:

- IP address,
 - browser type and version,
 - operating system,
 - pages visited,
 - time spent on the site,
 - traffic source (campaigns, social networks, search engines),
 - cookie identifiers.
- These technologies are used for functional, analytics and marketing purposes, as further detailed in our Cookie Policy.

c) Data related to campaigns and social networks

When you interact with our campaigns on platforms such as LinkedIn, Meta (Facebook and Instagram) or Google Ads, we may receive statistical or audience information and link it to your contact details if you complete a form or maintain a commercial relationship with us.

d) Sensitive data

Ctrl365 does not request sensitive data (such as health information, racial or ethnic origin, religious beliefs, political opinions, criminal records or personal financial information).

In some cases, such data might be received unintentionally (for example, content included in a CV or in a free-text field). In such cases, we will take reasonable measures to limit its processing, apply reinforced protection and delete it where appropriate.

4. Comments, media and embedded content

Although our primary focus is not an open-comments blog as in a standard CMS, it is possible that in certain areas of the Website we may enable the option to comment or upload content.

Comments

If a visitor leaves comments on the Website, we may collect the data displayed in the comments form, as well as the visitor's IP address and browser user-agent string, to help with spam detection and to maintain site security.

If we use external services such as Gravatar, an anonymized string (hash) may be created from your email address to check whether you use that service. Gravatar's privacy policy is available at: <https://automattic.com/privacy/>. After your comment is approved, your profile image, if applicable, may become public in the context of your comment.

Media

If we enable uploads of images or other files on the Website, we recommend avoiding content that includes location data (for example, EXIF metadata with GPS coordinates), as other users could extract such information from the files.

Embedded content from other websites

Some articles or sections of the Website may include embedded content (for example, videos, images, articles, widgets, third-party forms, etc.). Embedded content from other websites behaves in exactly the same way as if the visitor had visited the other website directly.

Those websites may collect data about you, use their own cookies, embed third-party tracking systems and monitor your interaction with that content, including tracking if you have an account and are logged in to that site. We recommend reviewing those third parties' privacy policies.

5. Purposes of processing

We use your personal data for specific, explicit and legitimate purposes, including:

- **Event, webinar and masterclass registration and management:**
To manage registrations, send reminders, share supplementary materials and post-event surveys.
 - **Sending commercial and marketing communications:**
To share information about solutions, case studies, relevant content and news, provided that you have given your consent or there is a legitimate interest consistent with the relationship.
 - **Managing resource downloads:**
To provide access to case studies, guides or other materials, and conduct commercial follow-up in line with the interest shown.
 - **Analytics and continuous improvement:**
To understand how the Website and our landing pages are used, optimize user experience and improve our campaigns using tools such as Google Analytics 4 (GA4) and Microsoft Clarity.
 - **Advertising and remarketing:**
To create custom audiences and display more relevant ads through platforms such as LinkedIn Ads, Meta Ads and Google Ads.
 - **Contractual and administrative management:**
Once the relationship progresses towards the provision of services, we may use your data to prepare proposals, contracts, invoicing and support.
 - **Compliance with legal obligations:**
To comply with requests from authorities, applicable regulations or internal audit and compliance processes.
- ## 6. Regulatory framework and legal bases by jurisdiction
- Ctrl365 applies the data protection regulations of each country in which we operate or where data subjects are located, and we process personal information only on the legal bases allowed by such regulations. In particular:
- **European Union (Spain):**
We fully apply Regulation (EU) 2016/679 (“GDPR”) and the supplementary Spanish regulations.
Legal bases include consent, performance of pre-contractual or contractual measures, legitimate interest and compliance with legal obligations.
 - **Argentina:**
We apply Law 25.326, its regulatory decree and the provisions of the Agencia de Acceso a la Información Pública (AAIP).
Legal bases include free, express and informed consent; legitimate interest linked to B2B activities; and contractual or pre-contractual needs.
 - **Mexico:**
We comply with the Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP) and its guidelines.
Legal bases include consent, pre-contractual/contractual relationship and legitimate compatible purposes.
 - **Colombia:**
We comply with Law 1581, its regulatory decrees and the guidelines of the Superintendence of Industry and Commerce (SIC).
Legal bases include prior, express and informed consent, as well as contractual or legal purposes.
 - **Chile:**
We apply Law 19.628 and the updates derived from the new Law 21.459 during its implementation process.
Legal bases include consent and legitimate purposes recognized by Chilean regulations.
 - **United States:**
Although there is no single federal data protection law, we adopt best practices aligned with frameworks such as CCPA/CPRA where applicable, especially for operations or users located in U.S. states with specific regulations.
 - **Rest of Latin America:**
We apply the local data protection laws of each country where our users or clients are located, respecting the legal bases admitted in each jurisdiction.

The GDPR only applies to data subjects located in the European Union or where European law is applicable due to the nature of the processing. However, as a corporate standard, we adopt good practices inspired by the GDPR, including principles of transparency, data minimization, security, accountability and continuous risk assessment.

7. Automation and AI

We use HubSpot as our CRM and marketing automation platform to segment contacts, perform lead scoring and manage campaigns. Some features may use AI-based algorithms to organize information or suggest segmentations.

These activities do not result in automated decisions producing significant effects on users. All relevant commercial interactions include human review. Such activities may be considered a form of profiling for strictly commercial and communication purposes.

We do not make decisions based solely on automated processing that produce legal effects or similarly significantly affect data subjects within the meaning of the GDPR or other applicable regulations. All relevant commercial decisions involve human intervention.

8. Recipients and data sharing

We may share your personal data only with the following types of recipients, to the extent necessary for the purposes described in this Policy:

- CRM and marketing automation providers (for example, HubSpot).
- Analytics and measurement providers (such as Google Analytics 4 and Microsoft Clarity).
- Digital advertising providers (such as LinkedIn Ads, Meta Ads and Google Ads).
- Infrastructure and cloud service providers that host or support our systems.
- Technology and security service providers (monitoring, backup, support, etc.).
- Technology and commercial partners in clearly informed joint activities (events, webinars, specific campaigns).
- External professional advisors (for example, law firms, accounting firms or auditors).
- Administrative or judicial authorities where there is a legal obligation to disclose data or where necessary to exercise our rights.

In all cases, we require these recipients to maintain the confidentiality of the information and apply appropriate security measures, acting under contracts that govern the processing of personal data.

9. International data transfers

Many of our technology providers operate globally and may process personal data in countries other than your own, including the United States and other territories.

When such transfers involve data belonging to individuals subject to the GDPR, we use mechanisms recognized by European law, mainly the Standard Contractual Clauses (SCCs) approved by the European Commission and, where appropriate, additional safeguards.

For users in Argentina and other Latin American countries, we carry out international transfers in accordance with articles 11 and related provisions of Law 25.326 and equivalent local regulations, using contracts with adequate guarantees or, where necessary, obtaining express consent.

We apply consistent security controls across all jurisdictions and require our providers to meet data protection standards aligned with international best practices.

10. Retention periods

Personal data is kept only for as long as necessary to fulfil the purposes for which it was collected, or for the period required by applicable law. As a general guideline:

- **Commercial leads and marketing contacts:** up to 36 months without relevant activity.
- **Event and webinar data:** up to 24 months after the activity has ended, unless there is a broader commercial relationship.
- **Active clients:** for the duration of the contractual relationship, plus any additional period required by accounting, tax or regulatory rules.
- **Analytics and cookie data:** according to the periods defined by each provider, as detailed in the Cookie Policy or in their own policies.

When data is no longer needed, it will be anonymised or securely deleted.

11. Data security

We have implemented technical and organizational measures designed to protect your personal information from accidental loss, unauthorized access, misuse, alteration or disclosure.

These measures include, among others:

- use of encryption protocols (such as TLS/SSL) for communications,
- strong password policies and restricted access,
- periodic security backups,
- role-based access controls,
- activity and audit logs,
- internal procedures for handling security incidents,
- infrastructure hosted with providers holding security certifications (for example, ISO 27001).

Our technology infrastructure is primarily hosted on Microsoft Azure, applying international security standards and other measures that may be defined together with our infrastructure and information security teams.

The security of your information also depends on you. If we provide you with credentials or you access restricted areas, you are responsible for keeping your password confidential and not sharing it with third parties.

Our infrastructure is mainly hosted on cloud services such as Microsoft Azure, which may operate in different regions and apply security controls aligned with international standards.

12. Your data protection rights

You may exercise your rights of access, rectification, update, deletion, objection, restriction and, where applicable, portability of your personal data by writing to legales@ctrl365.com.

To process your request, we may ask for information that allows us to verify your identity.

The exercise of rights is free of charge, and we will respond within the time limits set by the applicable regulations in each jurisdiction.

In Argentina, the competent authority for receiving claims under Law 25.326 is the Agencia de Acceso a la Información Pública (AAIP).

You may lodge a complaint with this authority if you believe your rights have not been adequately addressed.

Depending on your jurisdiction and place of residence, you may have the right to:

- request access to your personal data,
- request the rectification of inaccurate or incomplete information,
- request the deletion of your data when it is no longer needed or when you withdraw your consent,
- object to certain processing based on legitimate interest (for example, specific marketing activities),
- request restriction of processing in certain circumstances,
- and, in the case of the European Union, exercise the right to data portability.

Ctrl365 will not discriminate against any person for exercising their data protection rights.

If you wish to exercise these rights, or if you have questions about how we process your data, you can write to: legales@ctrl365.com. We may request additional information to verify your identity before responding.

13. Newsletters and commercial communications

In our forms, the sending of commercial communications and newsletters is carried out only when:

- you explicitly check the box to accept this type of communication, or
- there is a commercial or pre-contractual relationship that justifies this type of contact, always within the limits set by applicable law and respecting your preferences.

You can unsubscribe at any time by using the “unsubscribe” or “cancel subscription” link included in each email, or by requesting it at hi@ctrl365.com.

14. Minors

Our services and content are aimed at companies, professionals and organizations. We do not deliberately target minors, nor do we knowingly collect their personal data.

If we become aware that we have received information from minors without the appropriate consent, we will take reasonable steps to delete such data.

15. Changes to this Privacy Policy

We may update this Privacy Policy when necessary to reflect changes in legislation, our internal processes or the services we offer.

The current version will always be identified by the “Last updated” date at the beginning of the document. We recommend reviewing this Policy periodically. Continued use of the Website or our services after the publication of changes implies acceptance of the new version.

16. Acceptance

By using Ctrl365's services, the Website and/or our digital tools, you confirm that you have read and understood this Privacy Policy and agree that it is binding to the extent permitted by applicable law.

17. Contact information

For questions, comments or requests relating to this Privacy Policy and our data protection practices, you can contact us at:

- legales@ctrl365.com (main channel for privacy and data subject rights)
- hi@ctrl365.com (general company contact)

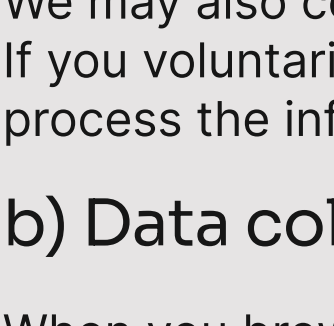
18. Job applications and CV submissions

The Website includes a dedicated space inviting interested individuals to send their curriculum vitae (CV) to the email address: recruiting@ctrl365.com.

The information contained in the CV will be used exclusively to assess the professional profile and, where applicable, to contact the applicant for future recruitment processes.

CVs will be stored for a maximum of 24 months or until you request their deletion by sending an email to legales@ctrl365.com.

We do not use online job application forms or automated CV processing on the Website.



COOKIE POLICY – Ctrl365

(separate version, 2026)

1. What are cookies?

Cookies are small text files stored on your device (computer, tablet, smartphone) when you visit certain websites. They are used to remember information about your browsing, improve user experience, provide additional functionality, perform analytics and display more relevant advertising.

We also use similar technologies (such as pixels or tags) that operate in a similar way to cookies.

2. Who is responsible for the use of cookies?

The controller responsible for the processing associated with the use of cookies on this Website is:

Ctrl365 S.A. – CUIT 30-71412704-3
Av. Leandro N. Alem 734, 5th Floor, C.A.B.A. (1001), Buenos Aires, Argentina
Contact: legales@ctrl365.com

3. Types of cookies we use

On our Website we use the following categories of cookies:

a) Strictly necessary cookies

These cookies are essential for the basic operation of the Website. They allow, for example, the site to display correctly, remember technical settings, enable security elements, manage form submissions and ensure indispensable operational functions.

They do not require your consent and remain always active, although you can manage them via your browser settings.

b) Functional or preference cookies

These cookies allow us to remember your preferences (such as language, region or certain display options) and improve your browsing experience. If you disable them, some functionalities may not be available or may not work as expected.

c) Analytics cookies

These cookies help us understand how the Website is used, which sections receive the most traffic, where visitors come from and how users interact with our content.

We use, among others, tools such as Google Analytics 4 (GA4) and Microsoft Clarity, which collect aggregated and anonymized information for statistical purposes and to improve the performance of the site.

These cookies are only activated if you give your consent through the cookie banner or cookie settings panel.

d) Marketing and advertising cookies

These cookies are used to show you more relevant ads and to measure the effectiveness of our campaigns. We may use, for example:

- LinkedIn Insight Tag
- Meta Pixel (Facebook/Instagram)
- Google Ads Tag

These cookies allow us to create audiences, perform remarketing and optimize our advertising activities.

4. Third-party cookies

Some cookies are set by third parties other than Ctrl365, in particular:

- analytics providers,
- advertising platforms,
- embedded content services (for example, videos, widgets or maps).

These third parties may carry out their own data processing in accordance with their own privacy policies, which we recommend you review. Where legally required, we will request your consent before enabling this type of cookie.

5. Managing your consent

When you visit the Website for the first time, you will see a cookie banner or notice that allows you to:

- accept all cookies,
- reject non-essential cookies,
- or configure your preferences by category.

We will only activate analytics and marketing cookies if you expressly accept them. You can change your choice at any time through the cookie settings panel available on the Website (for example, via a “Cookie settings” or similar link in the footer).

6. How to disable or delete cookies in your browser

In addition to our own settings panel, you can configure your browser to block, delete or limit the use of cookies. The procedures vary depending on the browser (Chrome, Firefox, Edge, Safari, etc.).

Please note that if you disable all cookies, the Website may not function correctly or some features may be affected.

7. “Do Not Track” and similar signals

Some browsers allow you to send “Do Not Track” (DNT) signals. Although there is currently no uniform standard for their interpretation, at Ctrl365 we comply with applicable regulations and complement these signals with our own cookie and consent management options.

8. Changes to this Cookie Policy

We may update this Cookie Policy to reflect legal, technical or service changes. The current version will always be the one published on the Website with its “Last updated” date.

9. Contact

If you have questions about the use of cookies or would like more information about how we process your personal data, you can write to: legales@ctrl365.com