DOITRIGHT CONSULTANTS

Privacy Policy

We don't collect your data. Period.

Effective February 27, 2026

🔒 **The short version:** Our apps do not collect, transmit, sell, or share any personal information from your device. No analytics. No crash reporting services. No advertising SDKs. No accounts required. What you do in our apps stays on your device.

1. Who We Are

DoITRight Consultants (**"DIRC"**, "we", "us", or "our") develops and publishes mobile applications for iOS, iPadOS, and Android. This Privacy Policy applies to all apps published under the **DoITRight Consultants** developer account on the Apple App Store and Google Play Store.

Questions about this policy can be directed to us at privacy@doitrightconsultants.com.

2. Apps Covered by This Policy

This policy covers all current and future DIRC mobile applications, including but not limited to:

APP	PLATFORM(S)	DESCRIPTION
IronPing	iOS / iPadOS	Network diagnostics toolkit (ping, traceroute, DNS, port test, HTTP/S, SMTP, SSH, WHOIS, GeoIP, subnet calculator)
ContactCleaner+	iOS / iPadOS	Contact management and deduplication utility

3. Information We Do Not Collect

Our apps are designed from the ground up to operate entirely on your device without sending data to DIRC or any third-party service we operate. Specifically, we do **not** collect:

- Your name, email address, phone number, or any contact details
- Your device's advertising identifier (IDFA / GAID)
- Location data
- IP addresses or network configuration of your device
- Browsing history, search history, or usage patterns
- Crash logs or diagnostic reports sent to DIRC servers
- Contacts, photos, files, or any other on-device content
- Any data typed or pasted into the app (hostnames, IP addresses, credentials, etc.)

- Behavioral analytics or heatmaps

We have deliberately excluded all third-party analytics SDKs, advertising networks, and telemetry frameworks from our apps.

4. How Our Apps Process Data Locally

All data you enter into our apps (hostnames, IP addresses, test results, saved hosts, workspaces, contacts) is stored exclusively on your device using Apple's on-device frameworks (SwiftData, Core Data, Keychain, UserDefaults). This data never leaves your device through our apps.

Some apps offer optional iCloud sync. When you enable iCloud sync, your data is synchronized between your own Apple devices through **your personal iCloud account**, governed by Apple's Privacy Policy. DIRC has no access to your iCloud data.

When you use network tools (e.g., ping a host, run a DNS lookup), the app makes outbound network connections directly from your device to the target hosts you specify. These connections are initiated solely by you and are not routed through or logged by DIRC servers.

5. Data Collected by Apple and Google

When you download, purchase, or update our apps through the Apple App Store or Google Play Store, those platforms may collect certain information as part of their standard operations. This data is collected directly by Apple or Google under their own privacy policies **— not by DIRC**.

Examples of what the platform stores may collect include:

- Purchase and download records (associated with your Apple ID or Google account)
- Crash reports and diagnostic data (if you have opted in to sharing with developers on your device)
- App usage metrics in aggregate (App Store Connect / Google Play Console analytics)
- Device type, OS version, and country/region (for aggregate, anonymized reporting)

DIRC may view aggregate, anonymized data provided by Apple App Store Connect or Google Play Console (e.g., total installs by country, average session length) solely for the purpose of improving our apps. This information cannot be used to identify individual users.

For more information, please review the platform privacy policies:

🍎 Apple Privacy Policy 📱 Google Privacy Policy

6. Children's Privacy

Our apps are not directed at children under the age of 13 (or the applicable minimum age in your jurisdiction). Because we do not collect any personal information, there is no risk of inadvertent collection of children's data through our apps. However, platform stores have their own policies regarding minors.

7. Your Privacy Rights

Because we do not collect or store any personal data on our own servers, there is no DIRC-held data to access, correct, export, or delete. All data you have saved within an app resides on your device and can be cleared at any time by deleting the app or clearing its data in your device settings.

If you are located in the European Economic Area, United Kingdom, California, or another jurisdiction with data privacy laws, please note that our no-collection approach already exceeds the requirements of those frameworks. You are always welcome to contact us with any questions or concerns at privacy@doitrightconsultants.com.

8. Security

Since we do not transmit or store your personal data on external servers, there is no DIRC-controlled data store that could be breached. On-device data is protected by your device's built-in security (passcode, Face ID / Touch ID, device encryption). Sensitive items such as SSH credentials are stored in the iOS Keychain, which is protected by Apple's hardware-backed security model.

9. Changes to This Policy

We may update this Privacy Policy from time to time. If we make material changes, we will update the effective date at the top of this page and, where appropriate, provide notice through our apps or website. Your continued use of our apps after any changes constitutes acceptance of the updated policy.

We will never change our core principle: **we will not collect, sell, or share your personal data.** Any future update to this policy will either maintain or strengthen these protections.

10. Contact Us

If you have questions, concerns, or feedback about this Privacy Policy or our apps, please contact us:

- **Email:** privacy@doitrightconsultants.com
- **Company:** DoITRight Consultants

We aim to respond to all privacy inquiries within five business days.

This policy was last updated on February 27, 2026.