Vtrack Link Service Privacy Policy

For Users in the Republic of Korea, the United States, Canada, and the EU/EEA

Last Updated: March 16, 2026

Effective Date: March 16, 2026

INTRODUCTION

This Privacy Policy (the "Policy") describes how Laon People Inc. ("Company," "we," "us," or "our") handles personal information in connection with the Vtrack Link application (the "App"). The App is a companion application designed exclusively to work with the Vtrack golf launch monitor hardware, enabling a local wireless connection between the launch monitor camera and the user's device for swing replay and analysis.

Our Core Principle — Zero Data Collection: The App does not collect, store, transmit, or process any personal information. All swing video data is processed locally on the user's own device via a direct local network (Access Point) connection with the Vtrack hardware. No data is sent to our servers, cloud services, or any third party.

This Policy is provided to ensure transparency and to inform users of their rights under applicable privacy laws, including the Republic of Korea's Personal Information Protection Act ("PIPA"), U.S. federal and state privacy laws, Canadian federal and provincial privacy laws, and the EU/EEA General Data Protection Regulation ("GDPR"). **The provision of this Policy does not constitute an admission that we are subject to any particular privacy law (except where such a policy is recommended or required by law, such as under the Republic of Korea's PIPA).**

We review and update this Policy at least once every **12 months**. If we make material changes, we will notify users through the App or our website prior to the changes taking effect.

PART A: INFORMATION WE DO NOT COLLECT

Section 1. Zero-Collection Architecture

The App is designed with a privacy-by-default and privacy-by-design architecture. We do **not** collect, receive, store, sell, share, or otherwise process any of the following:

- **Identifiers:** Name, email address, phone number, postal address, IP address, account credentials, or any other unique identifier.

- **Device Information:** Device model, operating system, unique device identifiers (IDFA/GAID), or hardware specifications.
- **Commercial Information:** Purchase history, payment information, or transaction records.
- **Internet/Network Activity Information:** Browsing history, search history, clickstream data, or interaction data.
- **Geolocation Data:** Precise or approximate location information.
- **Biometric Information:** Fingerprints, facial recognition data, voiceprints, or any physiological measurements.
- **Sensory Data:** Audio, visual, thermal, or olfactory information (swing video is processed locally on your device only — see Section 2).
- **Professional/Employment Information.**
- **Education Information.**
- **Sensitive Personal Information / Special Category Data:** Social Security numbers, driver's license numbers, racial or ethnic origin, religious or philosophical beliefs, health data, sexual orientation, political opinions, trade union membership, genetic data, etc.
- **Inferences or Profiles:** We do not create profiles, generate inferences, or perform any form of profiling or automated decision-making based on user data.

Section 2. How the App Works — Local Processing Only

The Vtrack Link App operates exclusively through a **local Access Point (AP) connection** between the Vtrack launch monitor and the user's PC or mobile device.

- **Data Flow:** Swing video captured by the launch monitor camera is streamed in real time to the user's device via a local wireless connection. This connection does not route through the internet, our servers, or any third-party infrastructure.
- **Replay System:** Swing replays displayed on the user's screen are processed in the device's local memory. Data is temporarily held during the session and is automatically cleared when the App is closed, unless the user manually saves it to their own device storage.
- **No External Transmission:** No feature of the App transmits user data to us or to any third party. We have no technical means to access, view, or retrieve any data from the user's device.

Section 3. No Tracking Technologies

The App does **not** use any of the following:

- Cookies, web beacons, or pixel tags
- Advertising identifiers (ADID, IDFA, GAID)
- Analytics tools or SDKs (e.g., Google Analytics, Firebase Analytics, Flurry)
- Crash reporting tools that transmit personal data
- Any third-party tracking or behavioral advertising technology

---

PART B: UNITED STATES — STATE PRIVACY RIGHTS

This Part applies to residents of U.S. states with comprehensive privacy laws. Because we do not collect personal information, the rights described below are fully satisfied by our zero-collection architecture.

Section 4. Your Rights Under U.S. State Privacy Laws

Depending on your state of residence, you may have rights under applicable state privacy laws, including but not limited to the California Consumer Privacy Act/California Privacy Rights Act (CCPA/CPRA), Virginia Consumer Data Protection Act (VCDPA), Colorado Privacy Act (CPA), Connecticut Data Privacy Act (CTDPA), Utah Consumer Privacy Act (UCPA), Texas Data Privacy and Security Act (TDPSA), Oregon Consumer Privacy Act (OCPA), Montana Consumer Data Privacy Act, Delaware Personal Data Privacy Act, Maryland Online Data Privacy Act (MODPA), Minnesota Consumer Data Privacy Act, New Hampshire Privacy Act, New Jersey Data Privacy Act, Iowa Consumer Data Protection Act, Indiana Consumer Data Protection Act, Kentucky Consumer Data Protection Act, Rhode Island Data Transparency and Privacy Protection Act, Nebraska Data Privacy Act, Tennessee Information Protection Act, and Florida Digital Bill of Rights:

1. **Right to Know / Right to Access:** You have the right to know what personal information we collect, use, disclose, or sell, and to request access to specific pieces of personal information. → *We do not collect any personal information.*
2. **Right to Delete:** You have the right to request deletion of personal information we hold about you. → *We do not hold any user data.*
3. **Right to Correct:** You have the right to request correction of inaccurate personal information. → *We do not hold any user data.*
4. **Right to Data Portability:** You have the right to obtain your personal information in a portable, readily usable format. → *We do not hold any data to provide.*
5. **Right to Opt-Out of Sale or Sharing:** You have the right to opt out of the sale of your personal information or its sharing for cross-context behavioral advertising. →

We do not sell or share any personal information. We have never sold or shared personal information. Accordingly, we do not provide a "Do Not Sell or Share My Personal Information" opt-out link.

6. **Right to Limit Use of Sensitive Personal Information:** → *We do not collect sensitive personal information. Accordingly, we do not provide a "Limit the Use of My Sensitive Personal Information" link.*
7. **Right to Opt-Out of Profiling / Automated Decision-Making:** → *We do not engage in profiling or automated decision-making.*
8. **Right to Non-Discrimination / Non-Retaliation:** You will not be discriminated against or subjected to retaliation for exercising any of the above rights.

Section 5. California-Specific Disclosures (CCPA/CPRA)

Categories of Personal Information — Past 12 Months:

CCPA Category	Collected	Sold	Shared for Behavioral Advertising	Disclosed for Business Purpose
A. Identifiers	No	No	No	No
B. CA Customer Records	No	No	No	No
C. Protected Classifications	No	No	No	No
D. Commercial Information	No	No	No	No
E. Biometric Information	No	No	No	No
F. Internet/Network Activity	No	No	No	No
G. Geolocation Data	No	No	No	No
H. Sensory Data	No	No	No	No
I. Professional/Employment Info	No	No	No	No
J. Education Information	No	No	No	No
K. Inferences	No	No	No	No
L. Sensitive Personal Info (SPI)	No	No	No	No

- **Sources of Personal Information:** None.
- **Business or Commercial Purpose for Collection:** Not applicable.

- **Data Retention and Deletion:** We do not retain any personal information. Session data (such as swing video) is automatically cleared when the App is closed. Any video manually saved by the user is stored solely on the user's local device, and we have no access to it. For information on how to exercise your deletion rights, please see Section 18.
- **Financial Incentives:** We do not offer financial incentives, price differences, or service-level differences in exchange for personal information.
- **Automated Decision-Making Technology (ADMT):** We do not use ADMT or engage in any profiling activities.
- **Global Privacy Control (GPC):** We respect GPC and other universal opt-out preference signals. However, as we do not collect, sell, or share personal information, no data processing activity is triggered or affected by such signals.

Section 6. Other U.S. State-Specific Notes

- **States requiring Universal Opt-Out Mechanism (UOOM) recognition** (including California, Colorado, Connecticut, Delaware, Maryland, Minnesota, Montana, New Hampshire, New Jersey, Oregon, and Texas): We acknowledge these requirements. As we do not collect or process personal information, there is no data processing activity subject to UOOM signals.
- **Applicability Thresholds:** Many state laws apply only to businesses that meet certain revenue or data processing thresholds. We do not currently meet such thresholds (e.g., CCPA's annual revenue threshold of $26,625,000 or the processing of personal information of 100,000 or more California consumers), nor do we collect personal information. This Policy is provided voluntarily for transparency.

PART C: CANADA — FEDERAL AND PROVINCIAL PRIVACY RIGHTS

This Part applies to users in Canada.

Section 7. PIPEDA (Personal Information Protection and Electronic Documents Act)

PIPEDA governs how private-sector organizations collect, use, and disclose personal information in the course of commercial activities across Canada. PIPEDA is built on **10 Fair Information Principles**, and our compliance is as follows:

1. **Accountability:** We have designated our Chief Technology Officer (CTO) as the officer responsible for privacy compliance (see Section 18).

2. **Identifying Purposes:** We do not collect personal information; therefore, no purpose identification is required.
3. **Consent:** As we do not collect personal information, no consent is required or sought.
4. **Limiting Collection:** We collect no personal information whatsoever — this principle is fully satisfied.
5. **Limiting Use, Disclosure, and Retention:** No personal information is used, disclosed, or retained.
6. **Accuracy:** Not applicable, as no personal information is held.
7. **Safeguards:** While we do not hold personal information, our App is designed to operate on a local, isolated network with no external data transmission capability, ensuring technical security by design.
8. **Openness:** This Policy constitutes our public disclosure of our privacy practices.
9. **Individual Access:** You have the right to request access to any personal information we hold about you. *We hold none.*
10. **Challenging Compliance:** You may challenge our compliance with PIPEDA by contacting our Privacy Team (see Section 18) or by filing a complaint with the Office of the Privacy Commissioner of Canada (www.priv.gc.ca).

Section 8. Quebec — Law 25

Quebec's Law 25 applies to any organization that handles personal information of Quebec residents, regardless of where the organization is located and with no minimum threshold.

- **Confidentiality by Default:** The App is designed with the highest level of privacy protection enabled by default. No tracking technologies are activated, and no personal information is collected.
- **Privacy Officer:** Designated (see Section 18).
- **Privacy Impact Assessments (PIAs):** As we do not collect, use, or disclose personal information, and do not transfer data outside Quebec (or anywhere), the triggers for PIAs under Law 25 are not activated.
- **Consent:** As no personal information is collected, no consent is required.
- **Data Subject Rights:** Quebec residents have rights including access, correction, deletion, de-indexation, objection to automated decision-making, and data portability. *As we do not hold any personal information, these rights are inherently satisfied.*

- **Data Breach Notification:** As we do not collect or store personal information, the risk of a data breach involving personal information is non-existent. In the unlikely event of any security incident, we will comply with applicable notification obligations under Law 25 and PIPEDA.
- **Cross-Border Transfers:** We do not transfer any personal information outside Quebec, Canada, or any other jurisdiction.

Section 9. Alberta (PIPA) and British Columbia (PIPA)

Alberta's Personal Information Protection Act and British Columbia's Personal Information Protection Act are provincial privacy laws deemed substantially similar to PIPEDA. Our zero-collection architecture satisfies the requirements of both laws.

Section 10. Canadian Users' Rights Summary

Regardless of your province or territory of residence, you have the following rights, all of which are inherently satisfied by our zero-collection design:

- Right to know what personal information we hold about you → *None*
- Right to access your personal information → *None held*
- Right to request correction of inaccurate information → *None held*
- Right to request deletion of your personal information → *None held*
- Right to withdraw consent → *No consent was required or obtained*
- Right to data portability (Quebec) → *None held*
- Right to file a complaint with the relevant privacy commissioner

---

PART D: EU/EEA — GENERAL DATA PROTECTION REGULATION (GDPR)

This Part applies to users residing in the European Union (EU) and the European Economic Area (EEA).

Section 11. Data Controller Information and Legal Basis

- **Data Controller:** Laon People Inc., 5F/6F, Building C, Gwacheon Urban Hub, 60, Gwacheon-daero 7na-gil, Gwacheon-si, Gyeonggi-do, 13840, Republic of Korea
- **Privacy Officer:** CTO
- **Privacy Team:** privacy@laonpeople.com / +82-1899-3058

- **EU Representative (GDPR Article 27):** GDPR Article 3(2) applies to the "processing of personal data" of data subjects in the EU in connection with the offering of goods or services. While we sell Vtrack launch monitor hardware in the EU/EEA, the App does not collect or process any personal information; therefore, the prerequisite of "processing of personal data" under Article 3(2) is not met. Additionally, the exemption under Article 27(2)(a) is satisfied, as any hypothetical processing would be occasional, would not include large-scale processing of special category data, and would be unlikely to result in a risk to the rights and freedoms of data subjects. Accordingly, we have not designated an EU representative at this time. Should any data processing activities arise in the future, we will immediately designate an EU representative and update this Policy. EU/EEA users may contact our Privacy Team directly at privacy@laonpeople.com.
- **Data Protection Officer (DPO):** Our CTO oversees privacy-related matters. We are not required to appoint a DPO under GDPR Article 37, as we do not engage in large-scale processing of personal data, special category data, or data relating to criminal convictions. Nevertheless, we have designated the above officer for privacy oversight. For inquiries, please contact our Privacy Team at privacy@laonpeople.com or +82-1899-3058.
- **Lawful Basis for Processing (Article 6):** We do not collect or process personal information; therefore, no lawful basis under Article 6 is applicable.

Section 12. Relationship to GDPR Principles

As the App does not collect or process personal information, the processing principles set out in GDPR Article 5 do not apply to any processing activity, because no such activity exists. For transparency, we provide the following overview:

1. **Lawfulness, Fairness, and Transparency:** We do not process personal data. This Policy ensures transparency.
2. **Purpose Limitation:** Not applicable (no collection).
3. **Data Minimisation:** The App collects no personal data whatsoever — this principle is fully satisfied.
4. **Accuracy:** Not applicable (no data held).
5. **Storage Limitation:** No personal data is stored. Session data is cleared upon App closure.
6. **Integrity and Confidentiality (Security):** The App operates on a local, isolated network with no external data transmission capability.
7. **Accountability:** This Policy and our internal technical documentation demonstrate our zero-collection design.

Section 13. EU/EEA Users' Rights Under the GDPR

Under the GDPR, EU/EEA residents have the following rights:

1. **Right of Access (Article 15):** → *No personal data is being processed.*
2. **Right to Rectification (Article 16):** → *No data is held.*
3. **Right to Erasure / Right to be Forgotten (Article 17):** → *No data is held.*
4. **Right to Restriction of Processing (Article 18):** → *No processing activity exists.*
5. **Right to Data Portability (Article 20):** → *No data is held.*
6. **Right to Object (Article 21):** → *No such processing activity exists.*
7. **Rights Related to Automated Decision-Making and Profiling (Article 22):** → *We do not engage in automated decision-making or profiling.*
8. **Right to Lodge a Complaint with a Supervisory Authority (Article 77):** You have the right to lodge a complaint with a supervisory authority in your member state of residence, place of work, or place of the alleged infringement.
9. **Right to Withdraw Consent (Article 7):** → *No consent was requested or obtained.*

Section 14. International Data Transfers

We do not transfer any personal information from the EU/EEA to any third country (including the Republic of Korea) or any other jurisdiction. All data processed by the App remains on the user's local device and does not pass through our servers.

Should any data transfer arise in the future due to service changes, we will implement appropriate safeguards under GDPR Chapter V (Articles 44–49), such as adequacy decisions or Standard Contractual Clauses (SCCs), and update this Policy accordingly.

Section 14-2. ePrivacy Directive

The EU ePrivacy Directive (2002/58/EC) governs the protection of personal data in electronic communications and requires consent for storing information on, or accessing information from, a user's terminal equipment. The App does not install cookies, trackers, or similar technologies on the user's terminal equipment, nor does it read or transmit any information from the terminal equipment to external parties.

> **Note:** In November 2025, the European Commission proposed the "Digital Omnibus Package," which includes proposed amendments to the GDPR, the ePrivacy Directive, the Data Act, and the EU AI Act. This proposal is currently under review by the European Parliament and the Council and has not been finalized. We will update this Policy upon final adoption of any relevant changes.

PART E: REPUBLIC OF KOREA — PERSONAL INFORMATION PROTECTION ACT (PIPA)

This Part applies to users residing in the Republic of Korea and is provided pursuant to Article 30 of the Personal Information Protection Act and Article 31 of the Enforcement Decree thereof.

Section 15. Purpose of Processing Personal Information

We do not process any personal information through the App. The App is a dedicated swing replay application that operates via a local AP connection between the Vtrack golf launch monitor and the user's device, and does not require the collection or use of personal information.

Section 15-2. Categories of Personal Information Processed and Retention Period

We do not process any personal information through the App; therefore, there are no categories of collected items and no retention or use period.

Section 15-3. Procedures and Methods for Destruction of Personal Information

We do not collect or retain personal information; therefore, there is no data subject to destruction. Swing video session data temporarily processed in the user's device local memory is automatically deleted when the App is closed, and we have no access to such data.

Section 15-4. Provision of Personal Information to Third Parties

We do not provide any personal information to third parties.

Section 15-5. Entrustment of Personal Information Processing

We do not entrust any personal information processing to external parties in connection with the App.

Section 15-6. Transfer of Personal Information Overseas

We do not transfer any personal information overseas through the App.

Section 15-7. Rights and Obligations of Data Subjects and Legal Representatives, and Methods of Exercise

Under the Personal Information Protection Act, data subjects (users) may exercise the following rights:

1. Right to request access to personal information
2. Right to request correction of errors
3. Right to request deletion
4. Right to request suspension of processing

→ *As we do not collect or retain personal information, there is no personal information subject to the above rights.*

If you wish to exercise any of the above rights, please contact our Privacy Officer or Privacy Team by mail, phone, or email as set forth in Section 15-9 below, and we will take prompt action.

Section 15-8. Automatic Collection Devices

We do not install or operate any automatic personal information collection devices, such as cookies, web beacons, or advertising identifiers (ADID/IDFA), in the App.

Section 15-9. Measures to Ensure the Security of Personal Information

Although we do not collect or retain personal information, we maintain the following safeguards for the safety of the App's operation pursuant to Article 29 of the Personal Information Protection Act and Article 30 of the Enforcement Decree:

- **Technical measures:** The App is designed to operate on a local, isolated network with no capability for external data transmission to our servers or third-party services, eliminating any technical pathway for personal information leakage.
- **Administrative measures:** We have designated a Privacy Officer and a Privacy Manager, and maintain internal procedures to review whether personal information processing is involved when App features are changed.
- **Physical measures:** As no data is collected or stored via the App, no separate physical storage devices or servers are operated.

Section 15-10. Privacy Officer and Privacy Manager

We have designated the following individuals to oversee personal information processing matters, handle data subject grievances, and provide remedies for damages:

Privacy Officer:

- Name: Gi-Wook Yoon
- Title: Senior Vice President / CTO
- Contact: +82-1899-3058 / privacy@laonpeople.com

Privacy Manager:

- Name: Hyun-Chang Choi
- Title: Team Lead
- Contact: +82-1899-3058 / privacy@laonpeople.com

> **Note for users outside the Republic of Korea:** In compliance with applicable laws in the United States, Canada, and the EU/EEA, which do not require disclosure of individual names of privacy officers, the Privacy Officer is identified as our CTO and the point of contact is our Privacy Team (privacy@laonpeople.com / +82-1899-3058) in the other Parts of this Policy.

Section 15-11. Remedies for Infringement of Data Subject Rights

Data subjects may contact the following organizations for dispute resolution, counseling, or other remedies regarding personal information infringement:

Organization	Contact	Website
Personal Information Dispute Mediation Committee	1833-6972 (no area code)	www.kopico.go.kr
Personal Information Infringement Report Center (KISA)	118 (no area code)	privacy.kisa.or.kr
Supreme Prosecutors' Office, Cyber Investigation Division	1301 (no area code)	www.spo.go.kr
National Police Agency, Cyber Investigation Bureau	182 (no area code)	ecrm.cyber.go.kr

Section 15-12. Changes to This Part

If any provisions of this Part are changed, we will post the changes through an in-app notice or on our website at least 7 days prior to the effective date. If material changes that significantly affect data subject rights are made, we will provide notice at least 30 days prior to the effective date.

PART F: GENERAL PROVISIONS

Section 16. Children's Privacy

We are committed to protecting the privacy of children. We do not knowingly collect personal information from anyone, including children.

- **United States:** In compliance with the Children's Online Privacy Protection Act (COPPA), we do not knowingly collect personal information from children under 13. Under California law (CCPA/CPRA), we do not knowingly sell or share the personal information of consumers under 16.
- **Canada:** In compliance with PIPEDA and applicable provincial laws, we do not knowingly collect personal information from minors.
- **EU/EEA:** Under GDPR Article 8, consent of a child for information society services requires parental/guardian authorization (age varies by member state, generally 13–16). As we do not collect personal information, no consent is required, and no children's data is at risk.
- **Republic of Korea:** Under PIPA, processing personal information of children under 14 requires consent of a legal representative. As we do not collect personal information, no consent is required, and no children's data is at risk.

Section 17. Third Parties

- We do not provide, sell, share, or disclose any personal information to any third party.
- The App does not integrate third-party analytics, advertising, or tracking SDKs.
- We do not participate in cross-context behavioral advertising or data broker activities.

Section 18. How to Exercise Your Rights / Contact Us

If you have any questions about this Policy, wish to exercise any privacy rights described herein, or have concerns about our data practices, you may contact us through the following methods:

- **Company:** Laon People Inc.
- **Address:** 5F/6F, Building C, Gwacheon Urban Hub, 60, Gwacheon-daero 7na-gil, Gwacheon-si, Gyeonggi-do, 13840, Republic of Korea
- **Privacy Officer:** CTO
- **Privacy Team:** Vtrack Link Support
- **Email:** privacy@laonpeople.com
- **Phone:** +82-1899-3058

- **Fax:** +82-2-3418-3351

For U.S. residents: We will respond to verifiable consumer requests within **45 calendar days** of receipt. If reasonably necessary, we may extend the response period by an additional 45 days (90 days total) with notice to you. You may designate an authorized agent to submit requests on your behalf; we may require written authorization or power of attorney.

For Canadian residents: We will respond to access or other privacy requests within **30 calendar days** of receipt, as required by PIPEDA and applicable provincial laws. If an extension is necessary, we will notify you.

For EU/EEA residents: We will respond to requests without undue delay and in any event within **one month (30 days)** of receipt. If a request is complex or numerous, we may extend the response period by an additional two months (three months total) with prior notice and explanation.

For Republic of Korea residents: We will respond to requests without delay in accordance with PIPA. Please refer to Section 15-10 for designated privacy officer contact information.

Filing Complaints:

Jurisdiction	Authority	Contact
Republic of Korea	Personal Information Dispute Mediation Committee	1833-6972 / www.kopico.go.kr
Republic of Korea	KISA Personal Information Infringement Report Center	118 / privacy.kisa.or.kr
U.S. (California)	California Privacy Protection Agency	www.cppa.ca.gov
U.S. (Other states)	Applicable State Attorney General	—
Canada (Federal)	Office of the Privacy Commissioner of Canada	www.priv.gc.ca
Canada (Quebec)	Commission d'accès à l'information du Québec	www.cai.gouv.qc.ca
Canada (Alberta)	OIPC Alberta	www.oipc.ab.ca
Canada (British Columbia)	OIPC British Columbia	www.oipc.bc.ca
EU/EEA	Data Protection Authority (DPA) in your member state	—

Section 19. Security Measures

Although we do not collect personal information, we maintain the following technical safeguards:

- The local AP connection between the Vtrack hardware and the user's device operates on an isolated local network that does not route through the public internet.
- The App contains no functionality for external data transmission to our servers or third-party services.
- Session data is processed in the device's local memory and is cleared upon App closure unless the user elects to save it locally.

Section 20. Changes to This Policy

We may update this Policy to reflect changes in applicable law, our services, or our practices. When we make material changes, we will provide notice through the App, our website, or other appropriate means prior to the effective date. The "Last Updated" date at the top of this Policy indicates when the most recent revision was made.

PART G: GOVERNING LANGUAGE

This Policy is provided in both Korean and English. In the event of any conflict or inconsistency between the two versions, **the English version shall prevail** for users in the United States, Canada, and the EU/EEA, and **the Korean version shall prevail** for users in the Republic of Korea.
