Checkin.com ID Verification Terms & Conditions

Effective Date: May 28, 2025

1. Purpose

These Terms & Conditions outline the requirements for an Identity Proofing Service Provider (IPSP), Checkin.com International AB, registered at Grev Turegatan 30, 114 38 Stockholm, Sweden (registration number 559352-2500) (Checkin.com), providing substantial identity verification of Users as a standalone service provider under Regulation (EU) No 910/2014 (eIDAS).

2. Scope

These conditions apply to Checkin.com to perform identity proofing of end-users at the substantial assurance level, as defined in eIDAS Implementing Regulation (EU) 2015/1502 and ETSI TS 119 461. Checkin.com provides services to relying parties requiring verified identities for electronic transactions. Checkin.com is assessed by an accredited Conformity Assessment Body and received an assessment report to demonstrate respective compliance. These Terms and Conditions are made available to all Users and Partners in accordance with ETSI EN 319 401.

3. Definitions

- **Identity Proofing**: The process of verifying the identity of a natural person to a substantial assurance level, ensuring a high degree of confidence in the claimed identity in accordance with ETSI TS 119 461 standards.
- **Substantial Assurance Level**: A level of assurance requiring significant evidence of identity in accordance with eIDAS requirements.
- **eIDAS**: Regulation (EU) No 910/2014 on electronic identification and trust services OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 for electronic transactions in the internal market and repealing Directive 1999/93/EC
- **ETSI EN 319 401**: General policy requirements for trust service providers.
- **IPSP Practice Statement**: The formal document issued by Checkin.com outlining its policies, procedures, and compliance measures for identity proofing services.
- **Services**: The identity verification and related services provided by Checkin.com under these Terms and Conditions, including but not limited to identity proofing processes, data processing, and delivery of verification

results to Partners, as described in the IPSP Practice Statement and in compliance with eIDAS and ETSI standards.

- **Partner**: A relying party, being an entity that contracts with Checkin.com to receive the Services for the purpose of verifying the identity of Users in connection with electronic transactions or services.
- **User**: A natural person whose identity is being verified by Checkin.com through the Services.

4. Data Protection and Security

4.1. Personal Data Protection:

Checkin.com shall implement technical and organizational measures to protect personal data used in identity proofing, ensuring compliance with Regulation (EU) 2016/679 (GDPR). These measures include data minimization, purpose limitation, and secure storage to prevent unauthorized access, profiling, or data breaches. Personal data shall only be processed for the purpose of providing identity proofing services at the substantial assurance level

4.2. Secure Authentication:

Identity proofing shall incorporate strong user authentication mechanisms, such as two-factor authentication based on at least two elements (knowledge, possession, or inherence), to meet the substantial assurance level.

6. Identity Proofing Methods

The approved methods and procedures for conducting substantial identity verification are outlined in the IPSP Practice Statement of Checkin.com.

7. Audit and Certification

7.1. Conformity Assessment:

Checkin.com has undergone an audit by an accredited Conformity Assessment Body (CAB) per ETSI EN 319 403-1 to verify compliance with eIDAS and ETSI TS 119 461 for substantial identity verification. The CAB has provided an assessment report confirming Checkin.com’s adherence to the required standards for an IPSP providing identity proofing services. The assessment report serves as evidence of compliance for relying parties. The assessment report is available to Partners upon request.

7.2. Vulnerability Assessment:

Checkin.com shall conduct vulnerability assessments every two years, addressing identified vulnerabilities within three months to maintain the validity of the assessment report.

8. IPSP Service Terms and Conditions

In addition to the terms and conditions of the service agreement to be concluded between Checkin.com and relying parties (the Service Agreement), the following terms apply to the identity proofing services provided by Checkin.com:

8.1. IPSP Practice Statement:

8.1.1. The trust service policy applied by Checkin.com for identity proofing services is detailed in the IPSP Practice Statement. The IPSP Practice Statement outlines the policies and procedures for providing identity proofing services at the substantial assurance level and is publicly accessible to all Users and Partners on Checkin.com's website.

8.1.2. Checkin.com shall maintain an IPSP Practice Statement describing its operational practices for identity proofing services. Policies and procedures for risk assessment and mitigation in identity proofing processes are regulated in the IPSP Practice Statement of Checkin.com.

8.2. Limitations on Service Use:

8.2.1 The use of the Services are limited by the use of a sufficiently enabled end user device, both when it relates to software such as browser versions and hardware camera quality. Minimum requirements are browsers built on Chrome 84 or Safari 13 and above. Internet Explorer (IE11) is not supported. Android native (app) use requires Android v10 or newer, iOS requires v12 or newer. The camera hardware supported requires a minimum of a HD capable camera with 1024x768 pixels or better with acceptable optic quality. Image quality acceptance is also part of the automatic checks and thus this requirement is also dependent on lightning and photographic qualities when using the Services.

8.2.2 The Services are limited to identity proofing at the substantial assurance level for use in electronic transactions by Partners. Checkin.com is not responsible for damages arising from use of the Services beyond their intended purpose, such as unauthorized reliance on verification results or use in non-compliant systems. The total liability for damages is capped as specified in Section 9 (Limitation of Liability).

8.3. Subscriber Obligations:

Users and Partners shall:

8.3.1. Provide accurate, complete, and up-to-date data for identity proofing

8.3.2. Notify Checkin.com immediately of any suspected compromise of authentication credentials or inaccuracies in verified data.

8.3.3. Use the Services in compliance with these Terms and Conditions and applicable laws, including eIDAS and GDPR.

8.4. Information for Relying Parties (Partners):

Partners can verify the identity proofing results by accessing the verification report provided by Checkin.com, which includes details on the User's identity, the verification method used, and the validity period of the verification. Partners should consult the IPSP Practice Statement for specific verification procedures and limitations.

8.5. Event Log Retention:

Checkin.com shall retain event logs related to identity proofing activities, including system logs, audit logs, and application logs, for a minimum period of 1 year unless a longer time is required by specific national regulations in the targeted country. These logs document significant events such as identity verification requests, authentication attempts, and service access, and are securely stored to prevent unauthorized access. PII connected to the event logs are removed based on the PII retention time set by the data owning Partner. PII will be deleted before the event logs are deleted if the PII retention time is less than 1year.

8.6. Contact Information:

For inquiries related to the Services, Users and Partners may contact Checkin.com at:

- **Address**: Grev Turegatan 30, 114 38 Stockholm, Sweden
- **Email**: support@checkin.com
- **Phone**: +46 8 123 456 78

8.7. Service Availability:

Checkin.com undertakes to provide a guaranteed level of service availability of at least 98% annually, excluding planned maintenance or interruptions beyond Checkin.com's control, such as force majeure events or third-party service failures. Details of the service level agreements (SLAs) are defined as part of the contractual agreement and may include higher availability figures.

8.8. Complaints and Dispute Settlement Procedures:

Checkin.com shall maintain procedures for handling complaints and disputes related to identity proofing services.

In Business-to-Consumer (B2C) scenarios, Users shall submit complaints directly to the Partner who contracted with Checkin.com for the identity proofing services.

In Business-to-Business (B2B) scenarios, Partners shall submit complaints via the general support email (support@checkin.com), which is processed through Checkin.com support ticketing system or other designated support channels, such as shared messenger systems.

9. Liability

9.1. Limitation of Liability:

9.1.1. SUBJECT TO THE PROVISIONS OF CLAUSE 9.1.2, THIS CLAUSE 9.1 SETS OUT THE ENTIRE FINANCIAL LIABILITY OF EITHER PARTY (INCLUDING ANY LIABILITY FOR THE ACTS OR OMISSIONS OF EITHER PARTY'S EMPLOYEES, AGENTS AND SUB-CONTRACTOR) IN RESPECT OF: ANY BREACH OF THIS AGREEMENT or SERVICE AGREEMENT; AND ANY USE MADE BY THE PARTNER OF THE SERVICES; AND ANY REPRESENTATION.

9.1.2. NOTHING IN THIS AGREEMENT LIMITS OR EXCLUDES EITHER PARTY'S LIABILITY: FOR FRAUD OR FRAUDULENT MISREPRESENTATION; OR FOR WILFUL MISCONDUCT; PAYMENT OF SUMS PROPERLY DUE AND OWING TO THE OTHER IN THE COURSE OF NORMAL PERFORMANCE OF THIS AGREEMENT; OR ANYTHING NOT PERMITTED TO BE LIMITED BY APPLICABLE LAW.

9.1.3. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CHECKIN.COM SHALL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, OR ANY LOSS OF PROFITS, REVENUE, DATA, OR USE, OR REPUTATIONAL HARM, WHETHER INCURRED DIRECTLY OR INDIRECTLY, OR ANY OTHER INTANGIBLE LOSSES, ARISING OUT OF OR IN CONNECTION WITH THE SERVICES, WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, OR OTHERWISE, EVEN IF CHECKIN.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE TOTAL AGGREGATE LIABILITY OF CHECKIN.COM FOR ALL CLAIMS ARISING OUT OF OR IN CONNECTION WITH THE SERVICES, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, SHALL NOT EXCEED THE TOTAL AMOUNT OF FEES PAID BY THE PARTNER TO CHECKIN.COM FOR THE SERVICES DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM.

10. Dispute Resolution:

Checkin.com has established a transparent and accessible dispute resolution process for handling complaints related to identity proofing errors or damages. Disputes shall be addressed through negotiation within 30 days of receipt of a

complaint. If unresolved, disputes shall be referred to a competent authority in accordance with the substantive laws of Sweden as stipulated in the Service Agreement.