

# Data Processing Agreement

Version 1.0 · Effective 10 October 2026

This Data Processing Agreement ("**DPA**") is made between:

1. **Wiretouch Ltd**, a company registered in England and Wales, trading as FacePing, of 71 Church Road, Hove, BN3 2BB, United Kingdom (the "**Processor**", "**FacePing**", "**we**" or "**us**"); and
2. the customer named in the Customer Agreement (the "**Controller**" or "**you**").

## 1. Incorporation and scope

1.1 This DPA forms part of, and is incorporated into, the agreement between the Controller and the Processor for the provision of the FacePing service (the "**Customer Agreement**"). By entering into the Customer Agreement, or by using the Service with real people after your application to go live is approved, the Controller agrees to this DPA.

1.2 This DPA applies to Personal Data that the Processor processes on behalf of the Controller in providing the Service. It does not apply to:

1. Personal Data that the Processor processes as a controller for its own purposes, such as customer account, billing, sign-up, application and website data, which is covered by the Processor's privacy notice at [faceping.ai/privacy](https://faceping.ai/privacy); or
2. the FacePing sandbox, where faces are enrolled, stored and matched only on the Controller's own devices and are never sent to the Processor. The sandbox is governed by the sandbox terms at [faceping.ai/terms](https://faceping.ai/terms).

1.3 This DPA is intended to meet the requirements of Article 28(3) of the UK GDPR and the EU GDPR, and the equivalent requirements of other Data Protection Law that applies to the processing.

## 2. Definitions

2.1 In this DPA:

1. "**Data Protection Law**" means all laws relating to data protection and privacy that apply to the processing of Personal Data under this DPA, including the UK GDPR, the Data Protection Act 2018, the EU GDPR and the national laws implementing or supplementing it, and, where relevant, US federal and state privacy and biometric privacy laws, including the Illinois Biometric Information Privacy Act ("**BIPA**"), the Texas Capture or Use of Biometric Identifier Act ("**CUBI**"), Washington's biometric identifiers law (RCW 19.375), the California Consumer Privacy Act as amended ("**CCPA**") and other US state consumer privacy laws ("**US State Biometric and Privacy Laws**"), each as amended or replaced from time to time.
2. "**EU GDPR**" means Regulation (EU) 2016/679.
3. "**UK GDPR**" means the EU GDPR as it forms part of the law of the United Kingdom under the European Union (Withdrawal) Act 2018, as amended.

4. "**Personal Data**", "**Special Category Data**", "**Processing**", "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data Breach**" and "**Supervisory Authority**" have the meanings given in the UK GDPR or EU GDPR (as applicable), and equivalent terms in other Data Protection Law (such as "biometric identifier", "biometric information", "business", "service provider" and "processor") are to be read accordingly.
5. "**Face Template**" means the numerical representation of a person's face that the Service creates from a photo. A Face Template is not a photo and cannot be turned back into a picture of the person, but it is biometric data used for the purpose of uniquely identifying a natural person, and so is Special Category Data.
6. "**Enrolled Person**" means a person whose Face Template is enrolled through the Service by or for the Controller.
7. "**Check-in List**" (or "**List**") means the container in the Service that holds a set of Enrolled People, such as a show, a festival, a gym's members, a workplace's staff or a list of visitors. A List either has an end date (a "**Dated List**") or has none (an "**Ongoing List**").
8. "**Check-in Device**" means a device paired with a List through a device token issued by the Controller.
9. "**Instructions**" has the meaning given in clause 5.1.
10. "**Service**" means the FacePing service, including the API, the dashboard at [app.faceping.ai](https://app.faceping.ai), the enrolment widget and the SDK, as described in the Customer Agreement and the documentation at [docs.faceping.ai](https://docs.faceping.ai).
11. "**Sub-processor**" means a third party engaged by the Processor to process Personal Data on behalf of the Controller.
12. "**Restricted Transfer**" means a transfer of Personal Data to a country outside the UK or the European Economic Area (as applicable) that requires a transfer mechanism under Data Protection Law.

2.2 Words such as "including" and "for example" do not limit the words that come before them.

### 3. Roles of the parties

3.1 For the Personal Data processed under this DPA, the Controller is the controller (or, under US State Biometric and Privacy Laws, the business or private entity that collects the data) and the Processor is the processor (or service provider) acting on the Controller's behalf.

3.2 Where the Controller is itself a processor acting for a third-party controller, the Controller warrants that its Instructions and its entry into this DPA are authorised by that third party, and the Processor is a sub-processor. The Controller remains the Processor's only point of contact and is responsible for passing on any notices or information to that third party.

### 4. Details of the processing

4.1 The subject matter, nature, purpose and duration of the processing, and the categories of Data Subjects and Personal Data, are set out in Annex A.

4.2 The processing includes Special Category Data (biometric data for the purpose of uniquely identifying a natural person under Article 9 of the UK GDPR and EU GDPR, and biometric identifiers or

information under US State Biometric and Privacy Laws).

4.3 The Service performs 1:1 verification by default: a face is compared only with the Face Template enrolled for the ID that the person presents. 1:N identification (comparing a face with all of a List's enrolled faces) is available only where the Processor has approved it in writing for the Controller's specific use case. Approval does not make the Processor responsible for the lawfulness of that use, which remains the Controller's responsibility.

## 5. Controller's instructions

5.1 The Processor will process Personal Data only on the Controller's documented instructions ("**Instructions**"), unless required to do so by UK law, the law of an EU member state or other law to which the Processor is subject. In that case the Processor will inform the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest.

5.2 The Controller's complete and final Instructions at the date of this DPA are: this DPA; the Customer Agreement; and the Controller's configuration and use of the Service (including its API calls, dashboard settings, List settings such as retention, enrolment widget settings and device tokens). Additional or different Instructions require the Processor's written agreement and may be subject to additional charges.

5.3 The Processor will tell the Controller promptly if, in its opinion, an Instruction infringes Data Protection Law. The Processor may suspend the affected processing until the Controller confirms, withdraws or changes the Instruction. The Processor is not obliged to perform a comprehensive legal examination of any Instruction, and informing the Controller is not legal advice.

5.4 The Processor will not:

1. process Personal Data for its own purposes, or for any purpose other than providing the Service to the Controller;
2. sell, lease, trade, rent, share for cross-context behavioural advertising, or otherwise profit from Personal Data, including any Face Template;
3. use Personal Data, including any Face Template or photo, to train, test or improve any face recognition or other machine learning model;
4. combine Personal Data with personal data it receives from or on behalf of any other person, or that it collects from its own interactions with Data Subjects, except as permitted by Data Protection Law; or
5. retain, use or disclose Personal Data outside the direct business relationship with the Controller.

5.5 For the purposes of the CCPA and similar US state laws, the Processor certifies that it understands and will comply with the restrictions in clause 5.4, and will notify the Controller if it determines that it can no longer meet its obligations under those laws. The Controller may, on notice, take reasonable and appropriate steps to stop and remediate unauthorised use of Personal Data.

5.6 The Processor may create and use aggregated, de-identified information that does not include any Face Template or photo and cannot reasonably be linked to any Data Subject (for example, counts of enrolled people used for billing, and service performance metrics) to provide, secure, bill for and improve the Service.

## 6. Controller's obligations and warranties

6.1 The Controller is responsible for its own compliance with Data Protection Law, and for the lawfulness of the processing it instructs. The Controller warrants, represents and undertakes that:

1. **Lawful basis.** It has, and will maintain throughout the processing, a lawful basis under Article 6 and a condition under Article 9 of the UK GDPR and EU GDPR (as applicable) for the processing, which for Face Templates will be the Data Subject's explicit consent unless the Controller has established, and documented, that another condition applies.
2. **Explicit consent.** Before any photo is submitted to the Service, it obtains each Data Subject's explicit, specific, informed, freely given and unambiguous consent (and, where the Data Subject is under 16, or under any higher age required by applicable law, the consent of a parent or guardian), records it accurately, and sends the Processor accurate consent information with each enrolment, including the consent text version the person saw. Where the Controller collects consent itself rather than through the enrolment widget, it uses the consent wording published by the Processor for the relevant version, or wording at least as protective.
3. **Privacy notices.** It provides each Data Subject, before enrolment, with a clear privacy notice that meets Articles 13 and 14 of the UK GDPR and EU GDPR and any other applicable notice requirement, including that the Processor processes the data on its behalf and where, and links to it in the Service settings.
4. **DPIA.** It carries out and documents a data protection impact assessment under Article 35 before its first use of the Service with real people, and before any material change in that use (including any use of 1:N identification), and consults the Supervisory Authority where Article 36 requires it.
5. **Alternative entry.** It offers, staffs and makes equally available for every List a way to check in that does not use face matching, and does not make face check-in a condition of buying a ticket, membership, employment or any other service, or treat people who decline it less favourably.
6. **Employees and imbalance of power.** Where the Data Subjects are its employees or others over whom it has a position of power, it has assessed whether consent can be freely given and ensured that refusal or withdrawal carries no detriment.
7. **US biometric laws.** For any List, venue or Data Subject in the United States, or where US State Biometric and Privacy Laws otherwise apply, it: (a) informs each Data Subject in writing, before collection, that a biometric identifier is being collected and stored, of the specific purpose and of the length of time for which it will be collected, stored and used; (b) obtains a written release (including an electronic signature where permitted) from the Data Subject or their legally authorised representative before collection, using the Processor's US release wording or wording at least as protective; (c) publishes, or ensures publication of, a written retention schedule and guidelines for permanently destroying biometric identifiers, consistent with the retention it sets in the Service; (d) does not sell, lease, trade or otherwise profit from biometric data; (e) complies with all notice, consent, opt-out, data minimisation, retention, security and assessment requirements of every other US State Biometric and Privacy Law that applies; (f) does not use the Service in any state or locality where its intended use is prohibited; and (g) sets the country of each List in the Service correctly. The Service chooses the consent wording it shows from the List's country (the US release wording for Lists in the United States), so the Controller is responsible for any List whose country is missing or wrong.

8. **Children.** It does not enrol children under 13 for any List in the United States, and does not enrol any child without the consent required by applicable law.
9. **Lawful collection.** Every photo it submits was collected directly from the Data Subject (or their guardian) through a consented enrolment flow. It does not submit photos taken from the internet, social media, CCTV or any other source, and does not use the Service to build a database of faces by untargeted collection.
10. **Permitted use.** It does not use the Service for covert identification, surveillance, tracking or monitoring of people, for scanning crowds, for inferring emotions, health, ethnicity, beliefs or other sensitive characteristics, for making decisions about a person based solely on their face, or for any use prohibited by Data Protection Law or by the Customer Agreement, and it uses 1:N identification only as approved under clause 4.3.
11. **Data subject requests.** It handles requests from Data Subjects, including withdrawals of consent and erasure requests, promptly, and uses the Service's tools to remove the person's enrolment.
12. **Accuracy of information.** All information it gives the Processor about the processing, including in its application to go live, is complete and accurate, and it will tell the Processor promptly of any material change.
13. **Staff and devices.** It ensures that its staff and contractors using the Service are trained, act lawfully and keep API keys, dashboard access and device tokens secure, and that it revokes devices and access promptly when they are lost, stolen or no longer needed.

6.2 The Controller is solely responsible for the choices it makes in the Service, including the retention period for each List, the content and timing of its privacy notices and consent flows, and decisions about who is admitted. The Service is a tool to assist check-in; the Controller remains responsible for any access decision and for having staff available to deal with failed or disputed checks.

## 7. Processor's obligations

7.1 The Processor will:

1. process Personal Data only on the Controller's Instructions, as set out in clause 5 (Article 28(3)(a));
2. ensure that persons authorised to process Personal Data are bound by confidentiality, as set out in clause 8 (Article 28(3)(b));
3. take all measures required by Article 32, as set out in clause 9 and Annex B (Article 28(3)(c));
4. respect the conditions for engaging Sub-processors in clause 10 (Article 28(3)(d));
5. assist the Controller with Data Subject requests, as set out in clause 12 (Article 28(3)(e));
6. assist the Controller with its obligations under Articles 32 to 36, as set out in clauses 9, 12 and 13 (Article 28(3)(f));
7. delete Personal Data at the end of the provision of the Service, as set out in clause 15 (Article 28(3)(g)); and
8. make available the information necessary to demonstrate compliance with Article 28 and allow for and contribute to audits, as set out in clause 14 (Article 28(3)(h)).

## 8. Confidentiality of personnel

8.1 The Processor will ensure that only personnel who need access to Personal Data to provide, support or secure the Service have access, that their access is limited to what they need, and that they are bound by a contractual or statutory duty of confidentiality.

8.2 To give support, the Processor's personnel may open the Controller's dashboard in a read-only support view. Each session lasts at most one hour, cannot change any data, is recorded in an audit log, and is listed for the Controller in the dashboard under Data & compliance, Support access. The support view does not display Face Templates.

## **9. Security**

9.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk to the rights and freedoms of natural persons, the Processor will implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including the measures in Annex B.

9.2 The Processor may update its technical and organisational measures from time to time, provided that the updated measures do not materially reduce the overall level of protection of Personal Data.

9.3 The Controller is responsible for the security of its own systems, accounts, API keys, device tokens and Check-in Devices, for the security of any photos and consent records it holds outside the Service, and for any security settings it chooses in the Service.

## **10. Sub-processors**

10.1 The Controller gives the Processor general written authorisation to engage Sub-processors. The current list is published at [faceping.ai/legal/sub-processors](https://faceping.ai/legal/sub-processors) and is incorporated in Annex C.

10.2 The Processor will notify the Controller of any intended addition or replacement of a Sub-processor at least 30 days before the new Sub-processor starts processing Personal Data, by email to the account owner's email address and by updating the published list.

10.3 The Controller may object to the change on reasonable grounds relating to data protection by writing to [support@faceping.ai](mailto:support@faceping.ai) within that 30-day period, giving its reasons. The parties will discuss the objection in good faith. If the Processor cannot reasonably accommodate the objection (for example by not using that Sub-processor for the Controller's data), the Controller may, as its sole and exclusive remedy, terminate the affected part of the Service by written notice before the change takes effect, and will receive a pro rata refund of any fees prepaid for the period after termination. If the Controller does not object within that period, it is taken to have accepted the change.

10.4 Where a change is needed urgently to protect the security or availability of the Service, or to comply with law, the Processor may make it on shorter notice. The Controller keeps its right to object under clause 10.3, running from the date of the notice.

10.5 The Processor will impose on each Sub-processor, by written contract, data protection obligations that offer at least the same level of protection for Personal Data as this DPA, to the extent relevant to the services the Sub-processor provides, including sufficient guarantees to implement appropriate technical and organisational measures.

10.6 Where a Sub-processor fails to fulfil its data protection obligations, the Processor remains liable to the Controller for the performance of that Sub-processor's obligations to the extent required by Data Protection Law, subject to clause 17.

10.7 Only Microsoft Azure, in the Controller's chosen region, stores Face Templates. No other Sub-processor stores Face Templates.

## **11. International transfers**

11.1 The Controller chooses the data region for its account (EU, which today is hosted in Microsoft Azure's North Europe region in Ireland; or the UK or US regions, which are available on request). Face Templates and consent records are stored only in the chosen region and are not transferred out of it for storage or processing at rest.

11.2 Check-in Devices download an encrypted copy of a List's Face Templates and hold it wherever the Controller uses them. The location of Check-in Devices is decided by the Controller, and any transfer that results from the Controller taking a device to, or using it in, another country is made by the Controller.

11.3 Traffic between people's browsers, Check-in Devices and the Service is routed through the Processor's content delivery and network security provider, and other limited data (such as customer account emails and billing information) is processed by Sub-processors listed in Annex C, which may involve Restricted Transfers. The Processor will ensure that every Restricted Transfer it makes is covered by a valid transfer mechanism under Data Protection Law, which may include: an adequacy decision or UK adequacy regulations (including the EU-US Data Privacy Framework and its UK Extension, where the recipient is certified); the EU Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914; the UK International Data Transfer Agreement; or the UK International Data Transfer Addendum to the EU Standard Contractual Clauses; together with any supplementary measures required.

11.4 Where the Controller is in the UK or EEA and the Processor is in the UK, the parties rely on the adequacy of the UK under the EU GDPR for transfers from the EEA to the Processor. If that adequacy ceases to apply, the parties agree that the EU Standard Contractual Clauses (Module 2, controller to processor) are incorporated into this DPA for those transfers, with clause 7 (docking) not used, option 2 of clause 9(a) (general authorisation, with the notice period in clause 10.2), the optional wording in clause 11 not used, Irish law and the courts of Ireland in clauses 17 and 18, and Annexes I to III completed from Annexes A to C of this DPA.

## **12. Assistance**

12.1 **Data Subject rights.** Taking into account the nature of the processing, the Processor will assist the Controller by appropriate technical and organisational measures, insofar as possible, to respond to requests from Data Subjects to exercise their rights. The Service lets the Controller list enrolled people and remove any person's enrolment at any time through the API and dashboard, which takes effect immediately on the server and on Check-in Devices at their next sync. If the Processor receives a request directly from a Data Subject that relates to the Controller's data, it will not respond to it (other

than to direct the person to the Controller, where it can identify the Controller) and will pass it to the Controller without undue delay.

**12.2 DPIAs and prior consultation.** The Processor will provide reasonable assistance to the Controller with data protection impact assessments and prior consultations with Supervisory Authorities, in each case to the extent the Controller does not otherwise have access to the relevant information and the information is available to the Processor. The Processor's DPIA template, security documentation and published product information form part of this assistance.

**12.3 Regulators and legal requests.** If the Processor receives a request from a Supervisory Authority, court or public authority concerning the Controller's Personal Data, it will, where legally permitted, inform the Controller promptly and cooperate with the Controller's reasonable instructions in responding. The Processor will disclose Personal Data to a public authority only where legally required to do so, and will challenge requests it considers unlawful.

**12.4 Costs.** Assistance provided through the Service's self-service tools and documentation is provided at no extra charge. The Processor may charge the Controller for its reasonable costs of any other assistance under this clause 12 or clause 13, except where the assistance is needed because of the Processor's breach of this DPA.

## 13. Personal Data Breaches

13.1 The Processor will notify the Controller without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach affecting the Controller's Personal Data. Notice will be given by email to the account owner and any data protection contact recorded in the Controller's account.

13.2 The notice will, to the extent the information is then available, describe:

1. the nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records concerned;
2. the name and contact details of the Processor's contact point where more information can be obtained;
3. the likely consequences of the Personal Data Breach; and
4. the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

13.3 Where it is not possible to provide all of that information at the same time, the Processor may provide it in phases without undue further delay.

13.4 The Processor will take reasonable steps to contain, investigate and mitigate the Personal Data Breach, and will provide reasonable cooperation to help the Controller meet its own obligations to notify Supervisory Authorities and Data Subjects. The Controller is responsible for deciding whether to notify, and for making, any notification to Supervisory Authorities, Data Subjects or others, and will not name the Processor in any such notification without consulting it first, except where required by law.

13.5 The Processor's notification of, or response to, a Personal Data Breach is not an acknowledgement of any fault or liability. A Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Personal Data, such as failed sign-in attempts, pings, port scans and denial of service attacks.

## **14. Records and audits**

14.1 The Processor will maintain a record of processing activities carried out on behalf of the Controller as required by Article 30(2), and will make it available to a Supervisory Authority on request.

14.2 The Processor will make available to the Controller, on written request, the information reasonably necessary to demonstrate compliance with this DPA and Article 28. The Controller agrees that this obligation will first be met by providing documentation, which may include this DPA and its annexes, the Processor's security documentation, its sub-processor list, answers to a reasonable written security questionnaire (no more than once a year), and the Controller's deletion log and support access log in the dashboard.

14.3 If the Controller reasonably considers that the documentation provided is not sufficient to demonstrate compliance, or where a Supervisory Authority requires it, the Controller (or an independent auditor it appoints who is not a competitor of the Processor and is bound by written confidentiality obligations) may carry out an audit, including an inspection, on the following conditions:

1. the Controller gives at least 30 days' written notice, with a proposed scope, which the parties will agree in good faith;
2. the audit takes place during normal business hours, does not unreasonably disrupt the Processor's business, and lasts no more than two working days on site, unless otherwise agreed;
3. no more than one audit takes place in any 12-month period, unless a Supervisory Authority requires it or the Controller has reasonable grounds to suspect a material breach of this DPA, including following a Personal Data Breach;
4. the audit does not give access to other customers' data, to information subject to legal privilege, or to information whose disclosure would compromise the security of the Service or breach the Processor's obligations to third parties;
5. audits of Sub-processors are satisfied by the information and audit reports the Sub-processor makes available; and
6. the Controller bears all its own costs, and pays the Processor's reasonable costs of supporting an on-site audit, unless the audit finds a material breach of this DPA by the Processor.

14.4 All information obtained in an audit is the Processor's confidential information, and the Controller will share any audit report with the Processor.

## **15. Deletion and return of Personal Data**

15.1 During the term, the Service deletes Face Templates and consent records automatically: (a) for a Dated List, at the List's deletion date (its end date plus the retention period the Controller chooses, from 0 to 30 days, with a default of 7 days); and (b) for an Ongoing List, for each Enrolled Person, when the maximum age the Controller chooses for the List (from 1 to 36 months, with a default of 12)

has passed since that person enrolled. Deletion happens earlier when the Controller removes an enrolment or deletes a List. Copies on Check-in Devices are deleted at the same time, even when offline, or when the Controller revokes the device.

15.2 On termination or expiry of the Customer Agreement, the Processor will delete all remaining Personal Data processed on behalf of the Controller within 30 days, unless UK law or the law of an EU member state requires its storage.

15.3 Face Templates are not returned. They are only usable within the Service, and returning biometric data would increase the risk to Data Subjects. Before termination, the Controller may export the list of enrolled people (their IDs, enrolment dates and consent versions) through the API or dashboard. The Controller agrees that deletion in accordance with this clause satisfies the Processor's obligation to delete or return Personal Data.

15.4 Deleted data may persist in the Processor's encrypted database backups until they expire on their normal rolling cycle, which will not exceed 35 days. Backups are not used to restore deleted Personal Data except to recover the Service after a disaster, in which case the Processor will re-apply all deletions that took place after the backup was made.

15.5 The Processor keeps a deletion log for each account, recording what was deleted, when and why. It contains no Face Templates, no ticket or person IDs and no record of who was deleted, and may be kept for the life of the Controller's account as evidence of compliance. On request, the Processor will certify in writing that deletion under clause 15.2 has taken place.

## **16. US State Biometric and Privacy Laws**

16.1 Where US State Biometric and Privacy Laws apply, the Processor will: process biometric identifiers and biometric information only as a service provider or processor for the Controller and only for the purpose of verifying the identity of Enrolled People at check-in; store, transmit and protect them using a reasonable standard of care within its industry, in a manner that is the same as or more protective than the manner in which it stores, transmits and protects other confidential and sensitive information; permanently destroy them in accordance with the retention the Controller sets, which cannot exceed 30 days after the end of a Dated List or 36 months after the person enrolled on an Ongoing List; and not disclose, redisclose or otherwise disseminate them except to Sub-processors needed to provide the Service under clause 10 or where required by law, a valid warrant or subpoena.

16.2 Nothing in this DPA makes the Processor responsible for obtaining any notice, consent or written release from Data Subjects, which is the Controller's responsibility under clause 6.

## **17. Liability and indemnity**

17.1 Each party's liability arising out of or in connection with this DPA, whether in contract, tort (including negligence) or otherwise, is subject to the exclusions and limitations of liability in the Customer Agreement, and the total liability of the Processor under this DPA and the Customer Agreement together will not exceed the limit set out in the Customer Agreement.

17.2 Nothing in this DPA limits or excludes either party's liability for death or personal injury caused by negligence, for fraud or fraudulent misrepresentation, or for any other liability that cannot be limited or

excluded by law, and nothing limits a Data Subject's rights against either party under Data Protection Law.

17.3 Each party is liable for its own breaches of this DPA and of Data Protection Law. Where both parties are responsible for the same damage, liability will be apportioned between them according to their respective responsibility for it, in accordance with Article 82 of the UK GDPR and EU GDPR.

17.4 The Controller will indemnify and keep indemnified the Processor, its officers and employees against all losses, liabilities, damages, fines, penalties, statutory damages, settlements, costs and expenses (including reasonable legal fees) arising from any claim, investigation or proceeding by a Data Subject, Supervisory Authority or other third party, to the extent arising from:

1. the Processor acting in accordance with the Controller's Instructions;
2. the Controller's failure to obtain any consent, written release or guardian consent, or to give any notice, required by Data Protection Law, including US State Biometric and Privacy Laws; or
3. any other breach by the Controller of clause 6 or of Data Protection Law.

17.5 The indemnity in clause 17.4 is subject to the Processor notifying the Controller promptly of the claim, not admitting liability without the Controller's consent (not to be unreasonably withheld), and allowing the Controller reasonable control of the defence, provided that the Processor may participate with its own counsel at its own cost and the Controller may not settle any claim in a way that imposes obligations on, or admits fault by, the Processor without its consent. The indemnity in clause 17.4 is not subject to the limitations of liability in the Customer Agreement, except where the Customer Agreement expressly says otherwise.

## 18. Term, precedence and general

18.1 **Term.** This DPA stays in force for as long as the Processor processes Personal Data on behalf of the Controller, and ends automatically when all such Personal Data has been deleted under clause 15. Clauses that by their nature are meant to survive, including clauses 15, 17 and 18, survive its end.

18.2 **Order of precedence.** If there is a conflict between this DPA and the Customer Agreement, this DPA prevails in relation to the processing of Personal Data. If there is a conflict between this DPA and any standard contractual clauses or transfer agreement incorporated into it under clause 11, the standard contractual clauses or transfer agreement prevail. Otherwise the Customer Agreement prevails.

18.3 **Changes.** The Processor may change this DPA by publishing a new version and notifying the Controller by email at least 30 days before a material change takes effect. The Processor may make a change immediately where it is required by law, by a Supervisory Authority, or by a change in a Sub-processor's terms that the Processor cannot control, in which case it will notify the Controller as soon as reasonably practicable. A change that does not materially reduce the protection of Personal Data may take effect on publication. If a material change has a material adverse effect on the Controller, the Controller may terminate the affected part of the Service by written notice before the change takes effect. Continued use of the Service after a change takes effect is acceptance of it.

18.4 **Severance.** If any provision of this DPA is found invalid or unenforceable, the rest of this DPA remains in effect, and the provision will be amended to the minimum extent necessary to make it valid

while keeping, as far as possible, the parties' original intention.

**18.5 Notices.** Notices to the Processor under this DPA must be sent to support@faceping.ai, or to Wiretouch Ltd, 71 Church Road, Hove, BN3 2BB, United Kingdom. Notices to the Controller will be sent to the account owner's email address.

**18.6 Third parties.** Except as required by Data Protection Law or any standard contractual clauses incorporated under clause 11, no person other than the parties has any right to enforce any term of this DPA, including under the Contracts (Rights of Third Parties) Act 1999.

**18.7 Governing law and jurisdiction.** This DPA, and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it, is governed by the law of England and Wales. The courts of England have exclusive jurisdiction to settle any such dispute or claim, except where Data Protection Law or standard contractual clauses incorporated under clause 11 require otherwise.

---

## Annex A: Details of the processing

| Item                        | Detail                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Controller                  | The customer named in the Customer Agreement. Contact details: as recorded in the customer's FacePing account.                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Processor                   | Wiretouch Ltd (trading as FacePing), 71 Church Road, Hove, BN3 2BB, United Kingdom. Contact: support@faceping.ai.                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Subject matter              | Face verification at check-in for the Controller's Lists (such as shows, venues, gyms and memberships, workplaces and visitor kiosks).                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Nature of the processing    | Receiving a photo of the person, with their consent information, at enrolment; creating a Face Template from it and discarding the photo; storing Face Templates and consent records; supplying encrypted, List-only copies of Face Templates to the Controller's Check-in Devices; on-device 1:1 verification, with liveness checks (1:N identification only where approved under clause 4.3); deletion at the end of the retention period (after a Dated List ends) or when each person's maximum age is reached (on an Ongoing List); logging deletions. |
| Purpose                     | Confirming that the person checking in is the person enrolled against the ID they present (for example their ticket, membership number or employee ID).                                                                                                                                                                                                                                                                                                                                                                                                     |
| Duration                    | For the term of the Customer Agreement. Each Face Template is kept until its Dated List's deletion date (end of the List plus 0 to 30 days, default 7) or, on an Ongoing List, until the List's maximum age has passed since the person enrolled (1 to 36 months, default 12), or until earlier removal, and all remaining data is deleted within 30 days of the Customer Agreement ending.                                                                                                                                                                 |
| Frequency                   | Continuous, for as long as the Controller uses the Service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Categories of Data Subjects | People the Controller enrolls for face check-in who have consented (or whose parent or guardian has consented), such as ticket holders, members, employees, contractors and visitors.                                                                                                                                                                                                                                                                                                                                                                       |
| Categories of Personal      | Face Template; the Controller's ID for the person (such as a ticket number, membership number or employee ID); consent record (consent text version, date and time of consent,                                                                                                                                                                                                                                                                                                                                                                              |

| Item                   | Detail                                                                                                                                                                                                                                                                                                                                                               |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data                   | whether a written release was given, whether the person is under 16 and whether a guardian consented, and how they were enrolled: widget, dashboard or API).                                                                                                                                                                                                         |
| Special Category Data  | Face Templates are biometric data processed for the purpose of uniquely identifying a natural person (Article 9 UK GDPR and EU GDPR), and biometric identifiers or information under US State Biometric and Privacy Laws. Restrictions and safeguards: those in Annex B, including encryption, region-pinned storage, strict access controls and automatic deletion. |
| Transient data         | The photo submitted at enrolment is held in memory only for as long as needed to create the Face Template, then cleared. It is never written to storage or logs. Camera frames used for verification on Check-in Devices are processed on the device and are not sent to the Processor.                                                                              |
| Data not required      | The Service does not need, and the Controller should not send, names, contact details or any other information about the person beyond the above.                                                                                                                                                                                                                    |
| Location of processing | Face Templates and consent records: the Controller's chosen region (EU: Microsoft Azure North Europe, Ireland; UK or US on request); copies on the Controller's Check-in Devices, wherever the Controller uses them. Network transit and other Sub-processors: as listed in Annex C.                                                                                 |

## Annex B: Technical and organisational measures

The Processor maintains at least the following measures. It does not currently hold any third-party security certification.

### Data minimisation

1. Photos are never stored. A photo is turned into a Face Template in memory and then discarded, and is never logged.
2. Consent is checked before a photo is decoded. Without valid consent information, the photo is not processed at all.
3. A Face Template is a list of numbers. It cannot be turned back into a picture of the person.
4. Only the information listed in Annex A is required. Deletion logs and billing records contain no Face Templates or person IDs.

### Encryption

5. All traffic between browsers, Check-in Devices and the Service uses TLS (HTTPS only).
6. Check-in Devices receive only their own List's Face Templates, as a pack encrypted with AES-256-GCM using a key for that List. On the device, Face Templates are stored encrypted with AES-256-GCM, and the key is held in the platform's secure storage (Keychain on iOS, Keystore on Android), never in the app's files.
7. API keys, device tokens, sign-in links and dashboard sessions are stored only as one-way hashes.

### Region and isolation

8. Each deployment serves one region (EU, UK or US). Face Templates and consent records are stored only in the Controller's chosen region and are not moved between regions.
9. Each customer can reach only its own Lists and data.
10. The API connects to its database with a least-privilege login limited to its own database, and network access to the database is restricted.

### **Access control**

11. Device tokens are limited to downloading a single List's Face Templates and can do nothing else. Each device has its own token, which the Controller can revoke at any time; a revoked device wipes its copy at its next sync.
12. Device copies carry a 24-hour lease: a device that cannot sync with the Service stops verifying after 24 hours until it syncs again. Devices sync automatically in the background.
13. The Processor's staff tooling is reachable only through single sign-on with named accounts, and every administrative action is recorded in an audit log.
14. Staff support access to a customer's dashboard is read-only, limited to one hour per session, logged, and shown to the customer (clause 8.2).
15. Rate limits apply to API keys, Check-in Devices and the enrolment widget.

### **Deletion and retention**

16. Retention is enforced automatically by a process that runs at least every 15 minutes: Face Templates and consent records are deleted at each Dated List's deletion date (0 to 30 days after the List ends, default 7), and on an Ongoing List each person's are deleted when the List's maximum age (1 to 36 months, default 12) has passed since they enrolled. The encrypted pack stops being served to devices at the deletion date, and a person past their maximum age is left out of every pack.
17. Check-in Devices delete their copy at the deletion date even when offline (checked when the app starts and on every verification), deleting the encryption key first and then the data. For an Ongoing List, each pack carries a deletion date no later than the earliest maximum age of anyone in it and no later than 30 days after the sync, so a device that stops syncing deletes its copy by then; the Service leaves out of each pack anyone whose maximum age falls within the device's 24-hour lease.
18. Removing an enrolment or deleting a List takes effect immediately on the server, and on devices at their next sync.
19. Every deletion is recorded in a deletion log: what, when and why, never who.

### **Accuracy and misuse prevention**

20. 1:1 verification by default. 1:N identification only where approved by the Processor, and it always returns a candidate for the person to confirm.
21. Liveness checks on every verification: passive liveness on every frame, failing closed, and an active check (a random head-turn challenge) on by default.
22. Face Templates from different models are never compared.
23. Every List must offer a way to check in without face matching; the Service will not create a List without one.
24. Each application to go live is assessed for its use case before real people can be enrolled.

## **Secure development**

- 25. Face detection, liveness, matching, encrypted storage and licence checks run in a native engine written in Rust, a memory-safe language, shared by the SDK and the server.
- 26. Face models are checked against known SHA-256 hashes on every build. Release builds cannot include test-only switches, and every package is checked for them before publication.
- 27. Third-party components and their licences are listed in the SDK's third-party notices.

## **Organisational**

- 28. Access to Personal Data is limited to personnel who need it, who are bound by confidentiality.
- 29. Sub-processors are engaged under written terms in line with clause 10.
- 30. Security issues can be reported to support@faceping.ai with "Security" in the subject; the Processor aims to reply within two working days.
- 31. Personal Data Breaches are handled and notified in line with clause 13.

## **Annex C: Sub-processors**

The Controller authorises the Sub-processors listed at [faceping.ai/legal/sub-processors](https://faceping.ai/legal/sub-processors), as updated from time to time under clause 10. That list sets out each Sub-processor's name, purpose, the data it handles, its location and the transfer safeguard used. Only Microsoft Azure, in the Controller's chosen region, stores Face Templates.