DETECTE

Detecte BV | BTW BE 1012.854.303
Dalemhof 87, 3000 Leuven, Belgium
W: https://www.detecte.eu/| E: Info@detecte.eu

DETECTE DATA PROCESSING POLICY

Last update: December 2025

Pursuant to the Agreement, Detecte provides the Solution and the Services (both as defined below) to the Customer (as defined below). The provision of the Solution and the Service leads to the collection and processing of Personal Data (as defined below) by Detecte, in its capacity as a data processor, on behalf of the Customer. Therefore, Detecte provides the Customer with this Data Processing Policy ("DPP") which sets out (i) how Detecte shall manage, process and secure the Personal Data; as well as (ii) all parties' obligations to comply with the Privacy Legislation (as defined below).

By concluding an Agreement with Detecte, the Customer has indicated that it has read, understands and accepts the terms and conditions of this DPP, which forms an integral part of said Agreement. Capitalised terms in this DPP shall have the same meaning as in the Agreement.

This DPP may be updated from time to time by Detecte, in which case Detecte shall notify the Customer through its Website (as defined below) or the Solution. In any event, the latest version of this DPP can always be accessed on the Website, as well as on the Solution.

1 DEFINITIONS

1.1 Capitalised terms shall have the meaning as set out below.

Assignment: All activities, performed by Detecte for the Customer, and any other form of cooperation whereby Detecte Processes Personal Data for the Customer, regardless of the legal nature of the agreement under which this Processing takes place;

Controller: The entity, which determines the purposes and means of the Processing of Personal Data, meaning the Customer as defined in the Agreement;

Customer: The party with whom Detecte has concluded the Agreement, including its Affiliate(s);

Data Subject: An identified or identifiable natural person where an identifiable natural person should be considered one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Detecte: The company Detecte BV, incorporated and existing under the laws of Belgium, with registered office at Dalemhof 87, 3000 Leuven, with VAT/company number BE-1012.854.303;

Personal Data: Any information relating to an identified or identifiable natural person (i.e. Data Subject);

Personal Data Breach: Unauthorised disclosure, access, abuse, loss, theft or accidental or unlawful destruction of Personal Data, which are processed by Detecte on behalf of the Customer;

Privacy Legislation The (supra)national privacy legislation applicable to the processing of personal data by the Customer or Detecte within the scope of the Agreement, such as, but not limited to: (i) the General Data Protection Regulation 2016/679 of April 27, 2016 ("GDPR"); (ii) United Kingdom (UK) Data Protection Act 2018; (iii) the Belgian Privacy Law of 30 July 2018; (iv) the ePrivacy Directive 2002/58/EC of 12 July 2002, including future amendments and revisions thereof; and/or (v) (future) national legislation regarding the implementation of the GDPR;

Processor: The entity which Processes Personal Data on behalf of the Controller;

Process/Processing: Any operation or set of operations which is performed upon Personal Data or sets of Personal Data, including but not limited to: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data;

Services: All services, provided by Detecte to the Customer with respect to the Solution (such as but no limited to support and maintenance);

Solution: The entire solution provided by Detecte, including the Hardware and the Software (as defined in the Agreement);

Sub-processor: Any Processor engaged by Detecte.

1.2 The Policy includes the following annexes:

Annex I: Overview of (i) the Personal Data, which parties expect to be subject of the Processing, (ii) the categories of Data Subjects, which parties expect to be subject of the Processing, the (iii) retention period for each Processing; and (iv) the use (i.e. the way(s) of Processing) of the Personal Data, the purpose and means of such Processing;

Annex II: Overview and description of the security measures taken by Detecte; and,

Annex III: List of Sub-processors engaged by Detecte.

1.3 The (uncapitalised) terms "(data) controller"; "personal data"; "personal data breach"; "process"; "processing"; "(data) processor" shall have the meaning attributed to them in the Privacy Legislation.

2 ROLES OF THE PARTIES

2.1 Parties acknowledge and agree that with regard to the Processing of Personal Data as instructed by the Customer, the Customer shall be considered 'Controller' and Detecte 'Processor'. Further, Detecte is allowed to engage Sub-processor(s) pursuant to the requirements set forth in Article 7.

2.2 Each party shall comply with its respective obligations under the Privacy Legislation with respect to the processing of the Personal Data.

3 USE OF THE APPLICATION AND/OR THE SERVICES

3.1 The Customer acknowledges explicitly that:

- ❑ Detecte purely acts as a facilitator of the Solution and/or the Services. Hence, the Customer shall be solely responsible on how and to what extent he/she makes use of the Solution and/or the Services as well as for all Personal Data collected through the Solution;
- ❑ It is responsible for all acts and omissions of Authorised Users (i.e. in case the Authorised User does (not) take sufficient measures to protect its account on the Solution);
- ❑ As a result of the use of the Solution, a number of connections between the Customer's technological infrastructure and the Solution shall be made. Data shall however only be uploaded upon approval of the Customer;
- ❑ It is responsible for the material and/or data provided by the Data Subject. The Customer is, as Controller, thus responsible for complying with the Privacy Legislation and/or any other regulations with regard to aforementioned material and/or data; and,
- ❑ It shall comply with all laws and regulations (such as, but not limited to: with regard to the retention period or rights of the Data Subject) imposed on it by making use of the Services.

3.2 The Customer shall avoid any misuse of the Solution and/or the Services. In case of misuse by the Customer of the Solution and/or the Services, the Customer agrees that Detecte can never be held liable in this respect nor for any damage that would occur from such misuse.

3.3 The Customer therefore undertakes to safeguard Detecte when such misuse would occur as well as for any claim from a Data Subject and/or third party due to such misuse.

4 OBJECT

4.1 Customer acknowledges that as a consequence of making use of the Solution and/or the Services of Detecte, the latter shall Process Personal Data as collected by the Customer. The nature and purpose of said processing, as well as a description of the Personal Data and categories of Data Subjects processed under the Agreement are further specified in Annex I.

4.2 Detecte shall always Process the Personal Data in a proper and careful way and in accordance with the Privacy Legislation and other applicable rules concerning the Processing of Personal Data.

4.3 More specifically, Detecte shall:

- ❑ during the performance of the Assignment – provide all its know-how in order to perform the Assignment according to the rules of art, as it fits a specialised and 'good' processor; and,
- ❑ shall adopt, to the best of its abilities, the necessary security measures (cfr. Annex II) and provide all its know-how in order to perform the Services in accordance with the rules of art.

4.4 The Customer keeps full control concerning the following: (i) how the Personal Data must be processed by Detecte; (ii) the types of Personal Data processed; (iii) the categories of Data Subjects whose Personal Data is subjected to the processing; (iv) the purpose of the processing; and (v) the fact whether such processing is proportionate.

4.5 This DPP is without prejudice to the provisions of the Agreement with regard to 'Data Protection'.

5 INSTRUCTIONS FROM / RESPONSIBILITY OF THE CUSTOMER

5.1 Instructions. Detecte shall only process the Personal Data upon the Customer's request and in accordance with the Customer's lawful instructions in Annex I, unless any legal obligation states otherwise. Detecte shall inform the Customer, if in its opinion, the instructions infringe the Privacy Legislation. If the Customer subsequently cannot guarantee the validity or legality of the instruction or fails or refuses to change the unlawful instruction so that it no longer violates the Privacy Legislation, Detecte shall be entitled to (i) suspend/refuse the performance of said instruction and (ii) at its discretion, to either continue to process the Personal Data in accordance with previously provided instructions or to stop the processing altogether, until the Customer has revised its instruction so that it no longer violates the Privacy Legislation.

5.2 Responsibilities. Furthermore, the Customer acknowledges that it is responsible for:

- ❑ the accuracy, quality and legality of (the collection and transfer of) the Personal Data;
- ❑ compliance with all transparency and lawfulness requirements under the Privacy Legislation for the collection and processing of the Personal Data and the transfer thereof to Detecte; and,
- ❑ ensuring compliance of its instructions (cfr. Annex I) with the Privacy Legislation.

5.3 Customer shall inform Detecte without undue delay if it is not able to comply with its responsibilities under this Section or the Privacy Legislation.

6 SECURITY OF PROCESSING

6.1 Detecte takes the security of the Processing activities very seriously. Detecte shall at least implement the technical and organisational measures specified in Annex II to ensure the security of the Personal Data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (Personal Data Breach). In assessing the appropriate level of security, Detecte and the Customer shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the risks involved for the Data Subjects.

7 SUB-PROCESSORS

7.1 Approval of Sub-processor list.

7.1.1 The Customer acknowledges and agrees that Detecte may engage Sub-processors in connection with provision of the Services (and the performance of the Agreement). In such case, Detecte shall ensure that the Sub-processors are at least bound by the same obligations by which Detecte is bound under this DPP.

7.1.2 Detecte has currently appointed as Sub-processors its Affiliates and other third parties as listed in Annex III.

7.1.3 Detecte shall be liable for the acts and omissions of its Sub-processors to the same extent as if it would be performing the Services/Processing of the Personal Data itself, directly under the terms of this DPP.

7.2 Update of the Sub-processor list.

7.2.1 Detecte shall:

- ❑ update the list whenever a Sub-processor changes (e.g. a new Sub-processor was added, a Sub-processor was substituted, etc.);
- ❑ clearly indicate the changes in the list; and,
- ❑ add a timestamp (i) when the list was updated, and (ii) when the change of the Sub-processor went or will go into effect.

7.2.2 Detecte shall notify the Customer (e.g. on the Website or through the Solution) when changes to the list are made.

7.3 Objection.

7.3.1 If the Customer wishes to exercise its right to object to a new Sub-processor, it shall notify Detecte in writing (cfr. Article 15) and based on reasonable grounds by the latest within thirty (30) days after the notification. If the Customer fails to object within the aforementioned timeframe it shall be deemed to have waived its right to object and to have authorised Detecte to engage the new Sub-processor.

7.3.2 In the event aforementioned objection is not found unreasonable by Detecte, parties will discuss the Customer's concerns with a view to achieving a reasonable solution. Such solution may include, at Detecte's discretion, to (i) make available to the Customer a change in the Services; or (ii) recommend a commercially reasonable change to the Customer's use of the Services to avoid the processing of the Personal Data by the objected new Sub-processor without unreasonably burdening the Customer.

7.3.3 If the parties are, however, unable to come to a solution within a reasonable period of time (which shall not exceed thirty (30) days following the objection of the Customer), the Customer may terminate the Services (in whole or partly) if:

- ❑ the Services/Solution cannot be used by the Customer without appealing to the objected new Sub-processor; or,
- ❑ such termination solely concerns that part of the Services which cannot be provided by Detecte without appealing to the objected new Sub-processor;

and this by providing written notice thereof to Detecte (cfr. Article 15) within a reasonable time.

7.3.4 Termination of the Services within the meaning of Article 7.3.3 shall be without liability to either party (but without prejudice to any fees incurred by the Customer prior to suspension or termination of the Services).

8 TRANSFER OF PERSONAL DATA OUTSIDE THE EEA

8.1 The Personal Data shall be processed within the European Economic Area ("EEA").

8.2 However, the Customer recognises that Detecte is entitled to transfer and store the Personal Data to countries outside the EEA for the purpose of providing the Services and fulfilling its obligations under the Agreement, and provided that such transfer/storage is done in accordance with the Privacy Legislation regarding additional safeguards. In particular, any transfer of Personal Data outside the EEA by Detecte to a third party whose domicile or registered office is in a country which does not fall under an adequacy decision enacted by the European Commission, shall be additionally subject to one or more of the listed EU-approved safeguards:

- ❑ European Commission Adequacy decision;
- ❑ closing a data transfer agreement: with the third country recipient, which shall contain the standard contractual clauses, as referred to in the 'European Commission implementing decision of 4 June 2021 (Decision (EU) 2021/914) on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council', including the performance of a transfer impact assessment. Before the transfer takes place, the recipient of the Personal Data/Sub-processor of Detecte in the third country has to guarantee Detecte that an adequate level of privacy compliance is ensured in this third party country;
- ❑ binding corporate rules: As it is the case for standard contractual clauses, the recipient of Personal Data/Sub-processor of Detecte in the third country has to guarantee Detecte that an adequate level of privacy compliance is ensured in the third party country; and/or,
- ❑ certification mechanisms.

8.3 In the event the transfer (or disclosure) of the Personal Data to a third country is required by EU law or EU member state law to which Detecte is subject to, Detecte shall inform the Customer of that legal requirement before the transfer/disclosure, unless that law prohibits such information on important grounds of public interest.

9 CONFIDENTIALITY

9.1 Detecte shall maintain the Personal Data confidential and thus not disclose nor transfer any Personal Data to third parties, without the prior permission of the Customer, unless when such disclosure and/or announcement is required by law or by a court or other government decision (of any kind). In such case Detecte shall, prior to any disclosure and/or announcement, inform you in full transparency on the scope and manner thereof.

9.2 Detecte shall ensure that its personnel, engaged in the performance of the Agreement, are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Detecte shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

9.3 Detecte shall ensure that its access to Personal Data is limited to such personnel performing the Assignment in accordance with the Policy.

9.4 The Customer acknowledges the login information to be strictly personal and ensures not to share this information with any third parties.

10 NOTIFICATION

10.1 Notification. Detecte shall use its best efforts to inform the Customer as soon as reasonably possible when it:

- ❑ receives a request for information, a subpoena or a request for inspection or audit from a competent public authority (incl. supervisory authority) in relation to the processing of the Personal Data;
- ❑ receives a request from a Data Subject invoking its privacy rights under the Privacy Legislation (cfr. Article 10.3);
- ❑ has the intention to disclose Personal Data to a competent public authority (incl. supervisory authority); or,
- ❑ determines or reasonably suspects a personal data breach has occurred in relation to the Personal Data.

10.2 Personal data breach. In case of a personal data breach, Detecte:

- ❑ shall notify the Customer without undue delay after becoming aware of this personal data breach and, to the extent possible, provide the information as required by Privacy Legislation (e.g. Article 33.3 GDPR). Upon request of the Customer, Detecte shall provide – to the extent possible – assistance with respect to the Customer's reporting obligation under the Privacy Legislation;
- ❑ undertakes – as soon as reasonably possible – to take appropriate remedial actions to make an end to the personal data breach (if such has occurred under its responsibility) and to prevent and/or limit any future personal data breaches.

10.3 Rights of Data Subjects.

10.3.1 Detecte shall promptly notify the Customer if it receives a request from a Data Subject invoking its privacy rights under the Privacy Legislation. Detecte shall not respond to any such Data Subject request without the Customer's prior written consent, except to confirm that the request relates to the Customer to which the Customer hereby agrees.

10.3.2 If a Data Subject requests to exercise his/her/their rights, it is the Customer's responsibility to assist the Data Subject in its request. Only if the Customer does not have the ability to correct, amend, block or delete the Personal Data (as required by Privacy Legislation), Detecte shall assist the Customer (as long as commercially reasonable and in line with applicable regulations).

10.3.3 Notwithstanding the foregoing, the Customer remains responsible for compliance of such Data Subject requests.

10.4 Data Protection Impact Assessment. Taking into account the nature of the processing and to the extent that (i) a data protection impact assessment is required under Privacy Legislation and (ii) the required information is reasonable available to Detecte and the Customer does not otherwise have access to said information, Detecte shall – upon request of the Customer – provide reasonable assistance to the Customer with the execution of a data protection impact assessment and possible prior consultation with the competent supervisory authorities. To the extent permitted by the Privacy Legislation, the Customer shall be responsible for any costs arising from Detecte' provisions of such assistance.

11 LIABILITY

11.1 Both parties are solely liable for all damage, claims and/or fines of third parties, competent supervisory authorities or Data Subjects that are the result of their own breach of or non-compliance with (i) the provisions of this DPP, and (ii) the Privacy Legislation or other applicable rules concerning Personal Data. Each party shall indemnify the other party in this regard.

11.2 In case of breach/non-compliance as described in Article 11.1 the infringing party is liable to the other party and must reimburse the latter for all damages and costs, including reasonable attorney's fees, (legal) expenses and damage resulting from such a breach/non-compliance.

11.3 In case of a proven breach by Detecte of its obligations under this DPP or under the Privacy Legislation, Detecte shall:

- ❑ be liable for the proven direct damages incurred by the Customer; and,
- ❑ not be liable for indirect, immaterial and/or consequential damages, including (but not limited to:) loss of profit, loss of opportunities, loss of and/or damage to data, loss of reputation, sanctions and/or fines, and unforeseeable damages.

11.4 Detecte's liability towards the Customer shall in any case be limited to the liability as set out in the Agreement.

11.5 The provisions in this Section shall be without prejudices to any other liabilities as agreed upon in the Agreement.

12 TERM

12.1 The total term of this DPP shall be the term of the Agreement. If no term is determined, this DPP shall remain in force as long as the Services has not come to an end.

13 RETURN AND DELETION OF PERSONAL DATA

13.1 Detecte shall only retain the Personal Data as long as needed to provide the Services or for the term of the Agreement (cfr. Article 12). The Customer accepts that Detecte may create back-ups of the Personal Data stored on the Solution.

13.2 Upon termination of the Services or the Agreement, the following shall apply:

- ❑ the Services and Solution shall be deactivated. Any Personal Data, stored on the Solution shall as from that moment no longer be available to the Customer;
- ❑ the Customer may request the Personal Data to be returned ('export') within thirty (30) days following the end of the Agreement or the Services, upon which Detecte shall assess whether such export is possible from a technical perspective. In any event, Detecte may, at its sole discretion, determine the format of the export. Detecte reserves the right to charge any costs relating to such exports to the Customer;
- ❑ after said thirty (30) days-period, the Personal Data on the Detecte Solution shall be deleted within one (1) month, unless it is required by applicable law to retain the Personal Data; and,
- ❑ the Personal Data may be present on back-ups. The Personal Data shall be deleted once the last back-up containing the Personal Data is rotated.

13.3 Please note that data or material provided to or submitted to Detecte by the Customer during the use of the Services may be further stored and processed by Detecte for further optimisation of the product and services following the termination of the Agreement or the Services. Detecte will never sell your data to third parties.

14 COMPLIANCE / INSPECTIONS

14.1 Compliance. Upon the Customer's request, Detecte shall make available to the Customer all information necessary and to the extent as requested by law to demonstrate its compliance with its obligations under this DPP.

14.2 Inspections.

14.2.1 Detecte shall allow the Customer (or a third party on its behalf) to carry out inspections – such as, but not limited to: an audit – and shall provide the necessary assistance thereto.

14.2.2 However, the Customer shall limit its initiatives to perform an inspection to a maximum of once a year. The Customer must notify Detecte at least thirty (30) working days in advance. The performance of inspections may in any case not cause any delay in the performance of the Services by Detecte.

14.2.3 The Customer shall impose sufficient confidentiality obligations on its (internal/external) auditors. As to ensure the confidentiality of other Customers, Detecte has the right to require from the Customer and its auditors to sign a non-disclosure agreement before the start of the inspection and to limit the scope of the inspection or the access of the Customers to certain premises.

14.2.4 All inspection costs are exclusively borne by the Customer, except if (and to the extent that) a severe security incident/personal data breach (at Detecte/under Detecte's responsibility) or a violation of this DPP is determined during the inspection.

15 NOTIFICATION / CONTACT DETECTE

15.1 Notifications by the Customer under this DPP and/or any questions or concerns with regard to the provisions of this DPP must be directed at simon@detecte.eu

16 MISCELLANEOUS

16.1 If one or more provisions of this agreement are found to be invalid, illegal or unenforceable, in whole or in part, the remainder of that provision and of this Agreement shall remain in full force and effect as if such invalid, illegal or unenforceable provision had never been contained herein. Moreover, in such event, Parties shall negotiate to replace the invalid provision by an equivalent provision in accordance with the spirit of this agreement. If Parties do not reach an agreement, then the competent court may mitigate the invalid provision to what is (legally) permitted.

16.2 Deviations, alterations and/or additions to this DPP shall only be valid and binding to the extent that they have been accepted in writing by both parties.

16.3 This DPP and the corresponding rights and obligations that exist in respect of the Parties, cannot be transferred, directly or indirectly, without the prior written consent of the other party.

16.4 (Repeatedly) non-enforcement by a party or by both parties of any right or provision of this DPP, can only be regarded as a toleration of a certain state, and does not lead to forfeiture.

16.5 This DPP prevails to any other agreement between the parties.

17 GOVERNING LAW & JURISDICTION

17.1 This DPP, including its Annexes, shall be governed by the law and subject to the jurisdiction clause as provided in the Agreement.

Annex I – INSTRUCTIONS OF THE CONTROLLER

I. DESCRIPTION OF THE PROCESSING ACTIVITIES

DRIVER & ACCOUNT MANAGEMENT

Purpose: Correct operation and support of the Service (managing accounts, rights, and licenses):

- Processing names, Driver ID, email addresses, and roles to authenticate and authorise the Customer's Authorised Users to access the sensitive Driver data and event logs.
- Linking the identity of the Driver (name, ID) to the purchased Subscription.

Data Subjects:
Personal Data:

✓ First name
✓ (Professional) E-mail address
✓ Personnel number
✓ Last name
✓ Role
✓ Log-in details (Driver ID and password)

Retention: Max. 3 months after termination of the Agreement.

DRIVER BEHAVIOUR, MONITORING AND SCORING

Purpose: Enhance road safety and prevent accidents. This is achieved by:

- Continuously monitor the Driver's attention levels. When distraction, smartphone use, or fatigue indicators are detected, immediate feedback is provided to the Driver to correct the behavior in real-time.
- The collected event logs (such as the frequency and severity of distractions) are transmitted to the Customer’s Dashboard. This enables the Customer to identify trends and risk profiles, allowing them to provide targeted coaching, training, and support their overall safety policies.

Data Subjects:
Personal Data:

✓ Drivers ID
✓ First name
✓ Personnel Number
✓ Last name
✓ Head/eye position of Driver
✓ Log-in details (Driver ID and password)

Retention:

- Head/eye position: 0 days (analysed instantly on device, not stored/transmitted).
- Event logs: 24 months after the date of the trip.

II. THE USE (= WAY(S) OF PROCESSING) OF THE PERSONAL DATA AND THE PURPOSES AND MEANS OF PROCESSING:

USE OF PERSONAL DATA

Ways of processing:

✓ Collect and store
✓ Structure and analyse
✓ Retrieve
✓ Consult
✓ Align, combine and create
✓ Transfer
✓ Update
✓ Erase and destroy

MEANS OF PROCESSING

Means:

✓ Solution
✓ Third party software (Sub-processors)
✓ Electronic communication
✓ Services

Annex II – TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

This document entails the technical and organisational security measures implemented by Detecte in support of its (Processing) activities, as set forth by the Privacy Legislation.

1 ORGANISATIONAL MEASURES AND ACCESS CONTROL

Security policy and governance

- Detecte maintains a comprehensive information security policy with attention to the core principles of confidentiality, integrity, and availability of data.
- The policy is periodically evaluated and refined during the further development of the Solution.
- Detecte executes appropriate Data Processing Agreements with all Sub-processors used or exclusively uses vendors that offer GDPR-compliant terms and conditions.

Access and password management

- Access to systems and Personal Data is strictly limited to authorised employees based on the “least privilege” principle (need-to-know basis).
- All internal accounts (Google Workspace, development environment, cloud services) are secured with mandatory Multi-Factor Authentication (2FA).
- A centralised password management tool is used for generating, storing, and managing unique passwords for each application or account to prevent credential reuse.

Confidentiality and awareness

- Personnel are bound by professional secrecy or a confidentiality clause.
- Involved employees are informed about privacy and security obligations and follow regular internal briefings regarding the secure handling of data.
- Access to Personal Data is strictly limited on a "need-to-know" basis.

2 TECHNICAL MEASURES

Cloud Infrastructure and Hosting

- The backend-infrastructure runs on Google Cloud Platform (GCP). GCP adheres to industry-leading security standards, including ISO 27001, SOC 2, and is certified as a GDPR-compliant data processor.
- GCP ensures redundant storage and automatic back-ups to guarantee availability and continuity.
- Access to backend environments is restricted via firewall rules, identity-based policies, and private endpoints (where possible).

Encryption and data security

- All communication between the Application, backend, and databases occurs exclusively via TLS 1.2+ encryption.
- Data stored by GCP is automatically encrypted with AES-256 encryption.
- Authentication attempts, API traffic, and platform events are logged for audit purposes and anomaly detection.

Application and device security

- Includes basis input validation on the server-side, use of modern frameworks, and regular updates of libraries and packages..
- Data temporarily processed on mobile devices is limited to the strictly necessary for real-time AI analysis. Data is not permanently stored locally on the device, unless functionally required.
- The processing of video images for AI analysis occurs exclusively locally on the mobile device in real-time, and no video footage is stored, recorded, or transmitted to the backend.

Security in design

- New functionalities are routinely assessed for privacy impact (Secure-by-Design approach)
- Code is managed via a centralizsd version control system with access control.
- Critical parts of the code are internally reviewed for quality and security.

Annex III – SUB-PROCESSORS

Detecte engages the following Sub-processors to assist in providing the Solution and Services:

Name	Nature of processing	Territory	Safeguard (if applicable)
Google Cloud Platform (GCP)	Hosting of backend, databases, logging, API's, and data processing infrastructure.	EU	N/A
Google Workspace	E-mail, internal document management, and internal communication.	EU/Worldwide	Adequacy decision: EU-US Data Privacy Framework