APPORTO'S GDPR Self-Certification Statement

(v. 1.0 – created 09.04.2025)

www.apporto.com

Apporto GDPR Self-Certification Document

Executive Summary

This document serves as a self-certification of our organization's compliance with the General Data Protection Regulation (EU) 2016/679 (GDPR). This certification covers our data processing activities, implemented safeguards, and ongoing compliance measures for the period specified above.

Certification Statement

We certify that, to the best of our knowledge and based on the assessments detailed in this document, our organization is compliant with the applicable requirements of the GDPR.

1. Data Processing Activities and Legal Bases

1.1 Data Processing Inventory

X **Complete** - We maintain a comprehensive record of all processing activities as required under Article 30 GDPR
☐ **In Progress** - Documentation is being updated
☐ **Not Complete** - Action required

Details: [Describe the scope of your data processing inventory]

1.2 Legal Bases for Processing

For each processing activity, we have identified and documented the appropriate legal basis:

X **Consent (Article 6(1)(a))** - Documented consent mechanisms in place
X **Contract (Article 6(1)(b))** - Processing necessary for contract performance
X **Legal Obligation (Article 6(1)(c))** - Processing required by law
X **Vital Interests (Article 6(1)(d))** - Processing to protect vital interests
X **Public Task (Article 6(1)(e))** - Processing for public interest tasks
X **Legitimate Interests (Article 6(1)(f))** - Legitimate interests assessment completed

1.3 Special Categories of Personal Data

X **N/A** - We do not process special categories of personal data
☐ **Applicable** - We process special categories under the following conditions:

- Article 9 legal basis identified: [Specify]
- Additional safeguards implemented: [Describe]

2. Data Subject Rights Implementation

2.1 Rights Management Framework

X **Right to Information** - Privacy notices provided at data collection
X **Right of Access** - Procedures established for subject access requests
X **Right to Rectification** - Process for correcting inaccurate data

X **Right to Erasure** - "Right to be forgotten" procedures implemented
X **Right to Restrict Processing** - Restriction mechanisms in place
X **Right to Data Portability** - Data export capabilities established
X **Right to Object** - Objection handling procedures implemented
X **Rights Related to Automated Decision Making** - Safeguards for automated processing

2.2 Response Procedures

- **Standard Response Time:** 30 days
- **Request Handling Process:** End-user will need to request personal user data review or deletion from the administrator at their higher education organization. Apporto does not have access to personal information outside of log-in and performance data. If log-in logs need to be deleted, the account administrator would open a ZenDesk ticket with Apporto.
- **Identity Verification:** Only the account administrator has the account log in information to be able to submit a ZenDesk ticket to Apporto.
- **Fee Structure:** None

3. Privacy by Design and Data Protection

Impact Assessments

3.1 Privacy by Design Implementation

X **Data Protection by Design** - Privacy considerations integrated into system design
X **Data Protection by Default** - Default settings protect personal data
X **Regular Review Process** - Ongoing assessment of privacy measures

3.2 Data Protection Impact Assessments (DPIAs)

X **DPIA Framework** - Process established for identifying when DPIAs are required
X **High-Risk Processing** - DPIAs completed for high-risk processing activities
X **Consultation Process** - Procedures for consulting supervisory authority when required

X **DPIA Register:** N/A - Determined due to size of company that DPIA is not required

4. Security of Processing

4.1 Technical and Organizational Measures

X **Encryption** - Data encrypted in transit and at rest where appropriate
X **Access Controls** - Role-based access controls implemented
X **Audit Logging** - Processing activities logged and monitored
X **Regular Testing** - Security measures regularly tested and evaluated
X **Staff Training** - Regular security awareness training provided

4.2 Security Incident Management

X **Incident Response Plan** - Documented procedures for security incidents
X **Breach Detection** - Monitoring systems for detecting personal data breaches
X **Notification Procedures** - 72-hour notification process to supervisory authority

X **Individual Notification** - Process for notifying affected individuals when required

Security Incidents: 0 incidents recorded in certification period
Breach Notifications: 0 notifications made to supervisory authority

5. International Data Transfers

5.1 Transfer Mechanisms

X **N/A** - No international transfers of personal data
☐ **Adequacy Decisions** - Transfers to countries with adequacy decisions
☐ **Standard Contractual Clauses** - EU SCCs implemented for transfers
☐ **Binding Corporate Rules** - BCRs approved and implemented
☐ **Certification Schemes** - Transfers under approved certification schemes
☐ **Other Safeguards** - [Specify alternative safeguards]

5.2 Transfer Risk Assessment

X N/A - **No international transfers of personal data**

☐ **Transfer Impact Assessments** - Risk assessments completed for transfers
☐ **Supplementary Measures** - Additional safeguards implemented where necessary
☐ **Ongoing Monitoring** - Regular review of transfer arrangements

6. Vendor and Third-Party Management

6.1 Data Processing Agreements

X **Processor Contracts** - Article 28 compliant contracts with all processors
X **Sub-processor Management** - Authorization and oversight of sub-processors
X **Joint Controller Arrangements** - Agreements defining responsibilities where applicable

6.2 Vendor Assessment

X **Due Diligence Process** - Security and privacy assessment of vendors
X **Regular Audits** - Periodic review of processor compliance
X **Incident Management** - Coordinated incident response with processors

7. Governance and Accountability

7.1 Organizational Structure

X **Data Protection Officer** - DPO appointed where required
X **Privacy Governance** - Clear roles and responsibilities defined
X **Senior Management Oversight** - Regular reporting to leadership

7.2 Documentation and Records

X **Processing Records** - Comprehensive records maintained per Article 30
X **Policy Documentation** - Privacy policies and procedures documented

X **Training Records** - Staff training completion tracked
X **Audit Trail** - Decision-making processes documented

7.3 Training and Awareness

X **Staff Training Program** - Regular GDPR training for all staff
X **Role-Specific Training** - Targeted training for data handling roles
X **Training Effectiveness** - Regular assessment of training outcomes

Training Completion Rate: 100% of staff completed GDPR training

8. Monitoring and Continuous Improvement

8.1 Compliance Monitoring

X **Regular Audits** - Internal audits of GDPR compliance
X **Performance Metrics** - KPIs for data protection compliance
X **Continuous Monitoring** - Ongoing assessment of compliance status

8.2 Improvement Actions

Identified Areas for Improvement:

1. Goal: Complete ISO27001 certification in 2026
2. Responsible party: Nahum Nicholas, Data Privacy Lead; Daniel Hutchison, CTO; Antony Awaida, CEO

Action Plan:

- Continue working towards ISO27001 certification with the creation of additional policies to be more fully compliant with ISO27001 requirements

9. Certification Declaration

9.1 Compliance Statement

Based on the assessments and evidence detailed in this document, we declare that:

1. We have implemented appropriate technical and organizational measures to ensure GDPR compliance
2. We have established procedures to handle data subject rights requests
3. We maintain adequate documentation of our processing activities
4. We have implemented appropriate security measures for personal data protection
5. We have established incident response procedures including breach notification
6. We provide regular training to staff on data protection requirements

9.2 Limitations and Disclaimers

This certification is based on our assessment, as of the certification date. We acknowledge that:

- GDPR compliance is an ongoing process requiring continuous monitoring
- Changes in processing activities, technology, or regulation may affect compliance status

- This self-certification does not constitute legal advice or guarantee regulatory compliance
- External audits or supervisory authority investigations may identify additional requirements

9.3 Review and Update Schedule

X **Quarterly Reviews** - Compliance status reviewed every 3 months
X **Annual Certification** - Full certification process repeated annually
X **Event-Driven Reviews** - Additional reviews triggered by significant changes

Next Review Date: August 12, 2026

Certification Approved by:

Name: Antony Awaida
Title: CEO

X

Antony Awaida

Signature: Signed by: 6131ff76-3ab9-472c-b7fa-fed75d5aa2b9

Date: 9/4/2025

Data Protection Lead Confirmation:

Name: Nahum A. Nicholas

Signature: Nahum Nicholas

Date: September 04, 2025