Security Policy

Last version: ***June 7, 2021***

Privacy and Information Security is our top-priority! We are happy to provide you with up-to-date information regarding our Data Processing activities and the Security Measures we have taken to protect Personal Data and other information.

Processing of Personal Data

We are Processing Personal Data as Processor on behalf of you (Customer) as Controller. The Processing activities might change due to Updates and Upgrades of Verifai Products and Services over time and might be Customer specific as described in the General Terms and Conditions - Including Data Processing Agreement (https://www.verifai.com/en/terms-and-conditions/). We are happy to provide more information about the Processing of Personal Data performed by Verifai.

The subject/nature and goal of the Processing:	Identity Verification Services
Description categories Personal Data:	• Personal data retrieved from Identity Documents; • Digital footprint • Biometric data (if applicable) • Contact details (if applicable) • Personal data retrieved from other documents (if applicable)
Description categories Data Subjects:	• End-users of Customer • Employees of Customer (via Account)
Description categories receivers of Personal Data:	• Verifai • Data center/hosting provider • Credit check agencies (if applicable) • Background check agencies (if applicable) • Technical Service Providers
Reasons for Processing:	Know your customer, customer due diligence, identity verification, age verification.

Location of Processing	• Verifai Products and Services
	  ○ Local processing on-device
	  ○ European Union
	  ○ United States (if applicable)

Sub-processors	• Payment Service Provider • Data Centers • Cloud provider (if applicable) • SMS Service Provider (if applicable)
Data Protection Officer	Verifai has appointed a Data Protection Officer (DPO) and officially registered the DPO under FG-number FG002607 at the Dutch Authority of Personal Data (Autoriteit Persoonsgegeves). Contact details: privacy@verifai.com

Security Measures

Verifai bears responsibility for ensuring the following technical security measures:

Compliance

ISO 27001	We are using ISO 27001 certified data centers located in the European Union. Verifai is working towards an ISO 27001 certification by a Certified Auditor for all Development and Data Processing activities.
GDPR	We are fully GDPR-compliant and we process personal data in accordance with the 'privacy by design' and 'privacy by default' principles. A Data Processing Agreement (DPA) is part of our General Terms and Conditions - Including Data Processing Agreement (https://www.verifai.com/en/terms-and-conditions/) when you are using Verifai Products and Services and DPAs have been closed with all relevant sub-processors. Thereby, we periodically conduct a Data Protection Impact Assessment (DPIA) to ensure that we assess the privacy risks. Interested in performing a DPIA for your own business processes? Learn more: https://support.verifai.com/hc/en-001/articles/360021697760-Data-Protection-Impact-Assessment-DPIA-information. On the other hand, we provide privacy filters and flexible data retention periods to secure and guarantee the privacy of your customer. Read our documentation: https://www.verifai.com/en/developers. More information can be found in our Privacy Policy (https://www.verifai.com/en/privacy-policy/).
Third-parties	We only contract third-parties for processing personal data which are ISO 27001 certified or SOC2 registered or certified which ensures a similar level of Information Security or higher.

Access Management

Access Management	Access to Verifai systems is based on 'Need-to-Know' and 'Need-to-Use' principles.

Employees

Screening	We control and monitor all our employees to ensure traceability around our office and equipment. Every employee has to comply with the general Verifai security roles and responsibilities. Thereby, all Dutch employees of Verifai have a declaration of good behavior (VOG) and signed an NDA before employment. In this case, we are sure that Verifai's code is developed under secure conditions.
Training and Assessments	All employees receive training and assessments within the first 3 (three) months after employment about information security and privacy.

Data Governance

Backups	We are making daily backups for our Verifai Products and Services.
Data Retention	Customers are responsible for setting the Data Retention Period for Processing Personal Data of End-users in all Verifai Products and Services. All Personal Data will be automatically erased after the Data Retention Period.

Information Security

Security Patches	We provide updates to resolve security vulnerabilities or security patches. As long as we are responsible for the security vulnerabilities, we will make an update available within 30 days after a written notification sent by the customer to security@verifai.com. However, if security vulnerabilities

	are upstream or caused by third parties, security patches will become available no earlier than the vendor has sent us the patches. No duration for these security patches is guaranteed.
Testing	We regularly perform a range of different security tests to ensure the security of all Verifai Products and Services, including but not limited to: penetration tests, vulnerability tests and functional tests.
Logging	All handlings are logged in our systems, which allows us to perform audits on a regular basis. We only process the digital footprint and scan information in the logs, no other personal data. All logs will be saved frequently on backups to guarantee evidence in possible court cases. We try to ensure full integrity and availability of the logs without any manipulation of the data.
Electronic Security	Verifai's dashboard and internal back office is fully protected to ensure strong passwords, among others, the following password requirements are at least included: • Users, admins and developers cannot use entire numeric passwords; • Passwords must be sufficiently different from certain attributes of the user; • Passwords are also checked against a list with 20,000 most common passwords in the world; • Passwords are always transmitted fully encrypted (hashed) and won't be visible during the login procedure (only obfuscations are used); • 2-factor authentication (2FA) is enforced and obligatory for Admin users; • Normal users can enable/disable 2-factor authentication (2FA) in the Verifai Dashboard; • A 48-hour rehearsal of the 2FA is enforced to ensure maximum protection.
Protection	The Dashboard, Platform and all Verifai Products and Services are protected by input validation, implementation of access control and restricting access to powerful database functions.

Physical Security

Physical Security	We are using modern identity and access management to highly secure our properties physically and electronically. Only authorized employees have access to specific systems and areas in the building. All authorizations are documented and carefully monitored to ensure a fully protected environment.

Policies and Procedures

Personal Data Breach(es)	When a data breach has been noticed, Verifai will notify the data breach ultimately within 72 hours to all affected parties by email in compliance with applicable law. Within 14 days after notification, a Risk Cause Analysis (RCA) will be sent to all affected parties
Hardening	To maximize security and minimize internal/external risks of attack, we are working continuously on the hardening of our policies. These hardening policies are updated over time to meet the most accurate standards and expectations.

Risk Management

OWASP	We perform OWASP assessment regularly and before we release updates or upgrades of our Verifai Products and Services.
DPIA	We perform Data Protection Impact Assessment (DPIA) periodically and before we release upgrades with new functionalities of our Verifai Products and Services.
Risk Assessments	We perform Risk Assessments periodically in accordance with the ISO 27001 standard.
Business Continuity	We have a Business Continuity Plan in place. The Business Continuity Plan is periodically tested.

Service Level	The Service Level Agreement is part of the General Terms and Conditions - Including Data Processing Agreement (https://www.verifai.com/en/terms-and-conditions/) .
Insurance	Verifai is insured for Third-Party loss and damage.

Policies and Procedures

Personal Data Breach(es)	When a data breach has been noticed, Verifai will notify the data breach ultimately within 72 hours to all affected parties by email in compliance with applicable law. Within 14 days after notification, a Risk Cause Analysis (RCA) will be sent to all affected parties

Digital Footprint

Cookies	We never use cookies in our SDKs and APIs. Our website only uses tracking cookies to monitor the conversion of our website. Learn more: https://www.verifai.com/en/cookie-policy/.