indaïa

TRUST & SECURITY

OUR APPROACH TO DATA SECURITY

Handling data is a huge part of our primary business, and we take personal data protection, privacy and security very seriously. The documents here explain how we handle data collected.

We have always been committed to invest in a continuous and growing security program since we first established Indaïa, and strive to go beyond the expectations.

Here are a few practical examples of security controls within our website:

- When synchronising devices with our secure online application, communication is over HTTPS and encrypted using TLS
- All non essential datas are stored for as short time as possible and are removed as soon as can be whilst retaining full functionality of the website.
- User access to Indaïa is secured with strong, complex authentication token and complexity controls are enforcable.
- We invest in scheduled, three-level penetration tests

GLOSSARY

For clarity, here are some terms we use in our security documents, and what they mean:

The Processor	Us, Indaïa
The Controller	You, Your Business
The Application	The Indaïa website

DATA OWNERSHIP, ACCEPTABLE USE & ACCESS TO COLLECTED DATA

Unambigously, the data you collect is your data and reserved solely for your own use.

Data and Personally Identifiable Information collected via our software is stored for the sole use of the Controller.

We facilitate the reliable collection and storage of data on our customers behalf, and our intentions will always be framed by this.

Some members of the Indaïa technical staff from time to time will have restricted access to the data we store on your behalf in order that we can carry out absolutely necessary service tasks such as the monitoring and improving the quality and performance of our own services, however under no circumstances any third-party able to access your data for any other purpose, such as marketing or communication purposes.

Data will never be disclosed to any third-party except in accordance with our Privacy Policy. The exceptions are:

- To provide a core feature or functionality which you request through the dashboard that depends on a third-party service.
- If we, or substantially all of our assets, are acquired or are in the process of being acquired by a third-party, in which case Personally Identifiable Information held by us, about our customers, will be one of the transferred assets.
- If we have been legitimately asked to provide information for legal or regulatory purposes or as part of legal proceedings or prospective legal proceedings.

COMPLIANCE & ACCREDITATIONS

Working with UK & European organisations

We fully comply and operate within the jurisdiction of UK and EU data law.

In light of the UK's potential withdrawal from the European Union in the coming years, we will continue to appraise the situation and adopt the most customer-favourable position on data security that we can achieve.

Working with US, UAE & other international organisations

As a company registered in France and storing data within the EEA, we are regulated by European laws which are widely considered more strict than many outside of the region.

Much of our compliance covers the core requirements of data law abroad, however we believe that European laws and the protection of rights of the individual and ownership of data currently provide the best protection of data anywhere worldwide.

If you are unsure about how this impacts your use of Indaïa, we suggest you seek additional legal advice. We generally find compliance teams find parity even where we do not comply to a specific foreign law.

Accreditations & Certifications

We continually and successfully work with data providers and organisations that already work within standardised frameworks such as ISO 27001, and we understand you may need to see accreditations as part of your assessment, we have gathered all the relevant documents for review directly here, in a reserved section.

Indaïa is working towards meeting it's own first international standards, so our current approach is to provide our own body of documents and policies that meet the requirements of organisations that do maintain these standards.

Our data is stored within certified facilities and our infrastructure built upon certified services.

Registration with the French Information Commissioner (CNIL)

We are members of the French Information Commissioner's Office (CNIL) Data Protection Register in France, and our registration number is **[LOLOLOLOL]**.

The Relationship Between You & Us

WHAT THE CNIL SAYS	IN PLAIN ENGLISH
The Controller collects and processes Personal Data in connection with its business activities.	You use Indaïa to collect data from your customers.
The Processor processes Personal Data on behalf of other businesses and organisations.	We manage that data for you.
Article 17(2) of the Data Protection Directive 95/46/EC provides that, where processing of Personal Data is carried out by a processor on behalf of a Controller, the Controller must choose a Processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures;	It is your responsibility to ensure our standards are good enough to meet your legal obligations and organisation's own standards. We are always willing to try to help you meet whatever data obligations are required in order to use our software.
Article 17(3) and 17(4) of the Data Protection Directive require that where processing is carried out by a Processor on behalf of a Controller such processing shall be governed by a contract or legal act binding the Processor to the Controller, stipulating, in particular, that the Processor shall act only on instructions from the Controller and shall comply with the technical and organisational security measures required under the appropriate national law to protection Personal Data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing;	We will manage the data in accordance with agreements we will make with you. These are outlined in our policies and terms and conditions when you sign up or start using our products. It is our responsibility to put measures in place to secure personal data you store with us.
The Processor takes all measures to protect Personal Data processed by the Processor on behalf of the Controller against a Security Incident and against all other unlawful forms of processing, as required under applicable national law. Such Technical and Organisational Security Measures shall include, as a minimum standard of protection, the following types of security measures: organisational controls, information security management systems; physical security; physical access controls; entry controls, virtual access controls, transmission controls, assignment of responsibility controls, availability and separation of responsibility controls, security and privacy enhancing technologies; awareness, training and security checks in relation to the Processor's Personnel; incident response management/business continuity; and audit controls/due diligence.	We are required to put in place measures to protect the data we store on your behalf at organisational, server and application levels.

DATA LIFE & DISPOSAL

Data Life, Retention & Protection

Data associated with your Indaïa account (including personal information and collected data) is retained for as long as you have a Indaïa account and for a longer period as may be required by law.

We don’t cancel accounts for inactivity.

You may delete your data from the website at any time.

- Data deleted in these ways will be made inaccessible but not permanently deleted - a ‘soft-deletion’, as permitted by law.
- We only retain your data to allow us to recover it should you accidentally delete it.
- We do eventually permanently erase old deleted data to reclaim storage space, we cannot guarantee that we will be able to restore deleted data.
- We do not use deleted data for any purpose other than to permit you the opportunity to restore it. Sometimes we may retain deleted data to comply with our legal obligations, resolve disputes, or enforce our agreements. In these cases, we ensure that access to such data is blocked except for the purposes for which we have been required to retain the information.
- It is the client’s responsibility to export and archive the data before the end of the 12 month period as we are not a data archival service, however this 12 month period is designed to help avoid any nasty surprises.

Permanent Deletion

To permanently delete data in the Indaïa website, click the Delete button and confirm. Once deleted from your account, you can contact us to request a permanent deletion of the soft-deleted data.

Backup Copies

Residual copies of data deleted from your account dashboard may remain on backup media as permitted by law. This data generally disappears after 12 months as old backup media gets overwritten with newer backups, which will result in total, permanent, unrecoverable deletion.

Hardware Management & Disposal

Computer equipment and storage media are destroyed beyond repair at their end of life. Our hosting provider shreds end-of-life hardware (although we are unable to provide certification for individual pieces of hardware), and we use secure erasure or destroy any storage media we use within the organisation.

All computer hardware and devices are issued centrally, and are logged in our central asset management system.

SERVERS & PHYSICAL LOCATION

Data centre location

The Data Centre is located in St. Ghislain in Belgium and is operated by Google. Google hold the following security related accreditations.

ISO/IEC 27001 - Security Management
ISO 22301 - Business Continuity Management
ISO 9001 - Quality Management
ISO 27017 - Cloud security
ISO 27018 - Cloud confidentiality
SSAE16/ISAE 402 TypeII (SOC 1, SOC 2, SOC 3)

Physical security

The Data Centre implements the following access controls at its premises and facilities:

- Secure monitored single-person entry
- All data is hosted in an off-site London data centre (operated by Google aswell)
- Independent client-card and biometric identification access system
- 24/7/365 manned security
- Firewalls and ACLs are in place to separate the trusted network from outside untrusted networks
- Administrative access is limited to only Google employees that need that level of access and physical and logical separation is in place to prevent access to trusted/internal networks
- Third parties i.e. contractors or suppliers not wholly controlled by the host have no operating system level or physical access to the infrastructure
- IDS, IPS, and logging are in-place and monitored 24x7 for alerts

How Personal Data Enters Our Software

Personal data enters Indaïa when an individual willingly enters their details via our platform, or if data is loaded into the Application via the Indaïa Dashboard or the documented Indaïa API.

THIRD-PARTY SERVICES

Some of our optional premium or custom product features require the use of third-party services outside of the EEA. Where we must work with third-party contractors or data services located in other jurisdictions, we prefer to work with companies that operate within government-backed schemes such as the EU-US Privacy Shield (previously Safe Harbor) scheme where possible.

Where possible we also always aim to anonymise data (decoupling it from the source) when transferring data to third parties.

We continually and successfully work with third-parties that already work within standardised frameworks and we understand you may need to see accreditations as part of your assessment.

"Amazon Privacy Notice" - Amazon
"What happens to my data" - Typeform
"Privacy Policy" - Airtable
"Privacy Policy" - Mailerlite
"Data Privacy" - Zapier

SERVICE FAILURE, BACKUPS & DISASTER RECOVERY

Servers

- Servers have UPS with backup diesel generators
- Trained engineers on-site 24/7/365 who can perform:
- Part swapping
- Fault diagnostics
- Software issue resolution - for servers, switches, firewalls and routers
- Server installation and racking

Backup schedule

- We conduct hourly data backups which are archived for one week
- We conduct daily data backups which are archived for one year
- We conduct weekly data backups which are archived for one week
- Hourly, daily and weekly backups are redundantly stored on our Google servers.
- We run continual real-time database replication within the same virtual private network
- Older, expiring backups are cyclically overwritten by newer backups

Please note, our businesss is not to act as a dedicated backup and archival service, so we always encourage our customers to use common sense and take sensible actions to make their own backup provisions in addition to the measures we take.

Disaster Recovery & Resiliance

Our comprehensive backup schedule and redundant, versioned, distributed backup means that in the event of a major disruption, we are in a strong position to recover very recent data and return servers to an operational state.

Our mobile and tablet apps work in offline mode when there is no good connection to our server, so if the main server hosted applications are offline, it will not affect any unsynchronised data on the apps.

POLICIES

Privacy Policy

- Our privacy policy is available here.
- We carry out an annual scheduled review of all privacy practices and policy at Indaïa to ensure up-to-date and appropriate practices

We will notify account owners by email if we make material changes to our privacy policy.

Privacy Compliance Violation & Remediation Policy

Any incident of privacy violation surrounding collected data is logged centrally and reviewed quarterly. Remediations will be proposed and timescales for implementation agreed and recorded in the log.

Staff Roles & Privilege Auditing

- We carry out an annual schedule of recorded, signed scheduled certification of user privileges to check correct permissions, and remediate any inconsistency
- We carry out a quarterly schedule of recorded investigation of user privileges for people with administrator rights to check correct permissions, and remediate any inconsistency

Emergency Staff Privilege Escalation Policy

Should we ever need to grant emergency privileges to internal or external personnel for any reason, this action is logged in our Emergency Access Log with full reasoning. We also log when those privileges are revoked.

Data Access Joiners, Movers & Leavers (JML) Policy

Staff privileges are assigned appropriate to their specific roles by senior staff members, and reviewed when employment ceases or when they change roles.

When a staff member leaves employment at Indaïa, we deactivate access to staff accounts as soon as we physically can, which is usually immediately. This deactivation always occurs within 48 hours of the end of their employment. Accounts are deleted within 30 days. All role changes are logged.

Network Security Policy

Any new system level components installed with vendor default settings in place are reset beforehand to remove risk of unsecure defaults.

Any redundant components, protocols, services and functions are shut down and removed as soon as technically feasible.

Any audit logs are established to be kept for a period of at least 1 year, with the last three months to remain immediately available.

Change Management & Change Control Policy

Change Control provides an orderly way to make changes to key process at Indaïa. It means notifying anyone affected by the change, and listening to the response should the change adversely affect team members or customers. It also means devising reasonable contingency plans for restoring the system if a change doesn't work.

By using a series of standardized and repeatable procedures and actions, we are able to introduce changes to the Indaïa infrastructure in such a way that any negative impact is minimized

This policy describes the process that is to be used for requesting and managing these changes. The following are the key roles specific to the Change Control process. One individual may be responsible for several roles as well as several individuals may be fulfilling a single role.

ROLE	DESCRIPTION
Change Control Manager	The Change Control Manager manages the process for all requests and reviews each request for completeness. The Change Control Manager verifies that the stated objectives of the request can be met and are consistent with company best practices. The Change Control Manager has the discretion to deny requests that are not consistent with company policy or best practices.
Change Requestor	The Change Requestor originates the request by submitting a change to the Change Control Manager.
Change Implementer	The Change Implementer makes the necessary changes as requested and notifies any other affected parties if corresponding changes need to be made. Changes are implemented into production by the Change Implementer.

Data & Information Classification Policy

All Indaïa team members share in the responsibility for ensuring the information assets we handle are given an appropriate level of protection by observing this Information Classification policy:

- Managers or information ‘owners’ shall be responsible for choosing classifications for information assets according to the information classification system below.
- Where possible, the information category shall be embedded in the information itself
- All team members shall use the information categories in their handling of security-related company information

All company owned information and information entrusted to us from third parties falls into one of four classifications:

CATEGORY	DESCRIPTION	EXAMPLES
Unclassified Public	Information is not confidential and can be made public without any implications for Indaïa. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.	• Product marketing information widely distributed • Information widely available in the public domain, including publicly available on the web site • Trial software • Financial reports required by regulatory authorities • Newsletters for external marketing
Proprietary	Proprietary Information is restricted to management-approved internal access, and protected from external access. Unauthorized access could influence Indaïa operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	• Passwords and information on corporate security procedures • Know-how used to process client information • Standard Operating Procedures used in all parts of Indaïa business • All Company-developed software code, whether used internally or sold to clients
Client Confidential Data	Information received from customers in any form for processing in production by Indaïa. The original copy of such information must not be changed in any way. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Data collected by customers • Electronic transmissions from customers • Product information generated for the customer by Indaïa production activities as specified by the customer
Company Confidential Data	Information collected and used by Indaïa in the conduct of its business to employ people, to log and fulfill customer requests, and to manage all aspects of company finance. Access to this information is restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Accounting data and internal financial reports • Confidential customer business data and confidential contracts • Non disclosure agreements with customers & vendors • Salaries and other personnel data • Company business plan

Email, Removable Media & Customer Data Transfer Policy

It is our policy that Customer Confidential data must not be sent via email or any publicly accessible electronic communication service without first being encrypted with a secure password that complies with our internal password policies. Data should only be transitted this way when other internal facing methods are not available. Passwords must be transmitted by a unassociated medium other than the medium the files are transmitted, such as via phone call.

We also do not ordinarily permit the storage or transfer of Customer Confidential data on removable media such as USB keys and external hard drives. Should it be necessary or unavoidable, any such data transferred or stored on removable media must be encrypted with a secure password that complies with our internal password policies.

Security Incident & Breach Reporting Policy

We maintain a centralised, fast, secure reporting system for the communication of all security and privacy issues. If a security or privacy issue is raised, a director of the business is immediately notified to co-ordinate the evaluation and necessary response, and the nature of the incident is logged alongside details, who is involved, actions taken and proposals for future action.

Should it be determined as necessarily significant during this evaluation, we will communinicate the nature of the security incident or breach to affected parties including customers as soon as we are able within the context of the situation, and in a manner which we believe will not exacerbate the worsening of the issue.

We will also notify the relevant authorities as soon as feasibly possible.

Clean Desk Policy

We run a clean desk policy at Indaïa. We do not print or handle phsyical copies of customer data at all if we can avoid it as we are primarily a digital operation, but in any rare instance when we should have to handle such documents, any such items will be stored in locked cabinets in the office overnight and securely destroyed on-site when no longer needed.

Software Update Policy

Application Updates are managed with a formalised version control flow, and go through a process of development team testing, wider internal testing (both automated and human), and pre-release testing with the live database

The final deployment of an Application update is automated and migrating to a new version requires no humanly noticeable downtime.

We update our servers with new patches on a monthly schedule. We also monitor for zero-day critical vulnerabilities and implement fixes within 24 hours or sooner where a patch is available.

More informations are available in our Development lifecycle document.

Policy Review Schedule

We review all of our internal policies on an as-needed basis, and also on a scheduled annual basis.