GDPR Policy

Nested Knowledge is committed to ensuring protection of all personal information that we hold. Nested Knowledge is located in the United States of America and provides services to users in countries across the world, except countries sanctioned by the U.S.

About GDPR

Key Terminology:

- **Personal data** - name, email, phone number, location data, appearance, customer id.
- **Sensitive personal data** - race, ethnitcy, religous or philosophical beliefs, political affiliation, health status, union membership, data concerning a person's sexual orientation or sex life, genetic data, and biometric data.
    - Biometric data uniquely identifies a person (e.g. facial id or fingerprint)
- **Controller** - Determines how data is processed.
- **Processor** - Processes data on behalf of another entity.
- **Subprocessor** - Processes data on behalf of another processor

Question: Who is the data subject, processor, controller, and subprocessor in this example?
Nested Knowledge orders buisiness cards for employees. A printing business, ACMEPrints, prints the business cards with the name and contact information of Nested Knowledge's employees. A cloud provider Cumulus Web Services hosts a database containing ACMEPrint's customers and their employees' contact information.

Answer: Nested Knowledge is the controller, the employees are the data subjects, ACMEPrint is the processor, and Cumulus Web Services is the sub-processor.

Scope: GDPR applies to the processing or controlling (by companies in ANY location) of personal data belonging to data subjects in the EU.

- A US company **processing data on its EU users** falls under GDPR, even when no payment is made for the company services
- A US company **handling data on employees and contractors in the EU** is bound by GDPR.
    - This includes non-residents and non-citizens physically located in the EU.

I. GDPR Data Processing

Nested Knowledge is committed to processing data in a lawful, fair, and transparent manner for explicit and legitimate purposes. Nested Knowledge will make all reasonable effort make sure data is accurate and up to date.

- **Sensitive Data** - Nested Knowledge does not process sensitive data (high-risk data) at this time.
- **Use of Photos** - User may voluntarily upload photos (see Photo Policy).

Technical and Organizational Measures (TOMS)

We have robust information security policies and procedures in place to protect personal information from unauthorized access, alteration, disclosure or destruction.

- **Testing** - Nested Knowledge frequently tests systems for data integrity. We undergo penetration testing annually (see Penetration Testing Policy), and our developers complete web security testing (see Security Awareness Training Policy) annually.
- **Security** - We encrypt personal data in transit and at rest.

Data Retention and Destruction

Personal information is stored, archived and destroyed in accordance with our service and regulatory obligations. Data is deleted when it is no longer needed.

- Internal personal data: refer to our Document Retention Policy.
- Personal data of users (in which Nested Knowledge acts as processor), see our Backup Procedures.

Record of Processing Activities

Nested Knowledge maintains a Record of Processing Activities (ROPA) describing the data categories, purpose, data subjects, legal basis, retention period, and security measures about the data that we control and process.

II. Data Protection Impact Assessment

Before processing personal information that may result in a high risk to data subjects, Nested Knowledge employees will undergo a Data Protection Impact Assessment (DPIA), as described in our Data Protection Policy.

Question: a new Marketing intern would like to target LinkedIn Ad campaigns based on customers' political affiliation, derived by analyzing public voting records. Can the intern do so?
Answer: No, political affiliation is sensitive personal data. To consider proceeding, the marketing team must complete and document a DPIA that evaluates the lawful basis for processing, potential harms, risk reduction, and other details.

III. Privacy Policy and Data Subject Rights

OurPrivacy Policy ensures that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information. Nested Knowledge will use 3rd party compliance service to stay updated with privacy regulation changes.

Our Privacy Policy was first published online on January 3rd, 2022 and last updated on **May 16, 2023.**

Data Subject Rights

Individuals have a right to access any personal information that Nested Knowledge processes about them and to request information about:

- what personal data we hold about them
- the purposes of the processing
- the categories of personal data concerned
- the recipients to whom the personal data has/will be disclosed
- how long we intend to store your personal data for
- if we did not collect the data directly from them, information about the source
- the right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- the right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- the right to lodge a complaint or seek judicial remedy and who to contact in such instances.

Nested Knowledge provides easy-to-access information via our Privacy Policy. We can be reached for further inquiry through our Data Protection Officer.

IV. Consent and Notices

Obtaining Consent

We have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information.

- **Direct Marketing** - Our direct marketing includes clear opt-in mechanisms for marketing subscriptions and a clear notice and method for opting out on all subsequent marketing materials.
- **Cookies** - We do not use marketing or analytics cookies.

Communicating Updates

As described in our Third Party Policy, we will notify user of significant changes to how their data is processed, such as the addition of a new subproccesor, at least 7 days in advance.

Reporting Data Breaches

Nested Knowledge is obligated to report information on data breaches and mitigations to the required government agencies as well as reporting information of data breaches to the affected parties. Our Incident Response policy ensure that we have safeguards in place to identify, assess, investigate and report any personal data breach as early as possible. We inform clients of breaches in accordance with our Escalation Policy.

V. Statement on Subprocessors

As described in theThird Party Policy Nested Knowledge maintains a List of Subprocessors and Third Party providers. We update the list on an ongoing basis when a change in subprocessors occurs.

New contracts with subprocessors and subcontractors will incorporate data protection and data breach notice requirements.

VI. GDPR Roles and Accountability

- **Data Protection Officer** - See the Data Protection Officer section of our Information Security policy. Nested Knowledge's Data Protection Officer is responsible for promoting awareness of the GDPR across the organization, assessing our GDPR compliance, identifying any gap areas and implementing the new policies, procedures and measures
- **Employee Training** - Nested Knowledge trains employees on GDPR compliance at least annually
- **GDPR Audit Record -** Nested Knowledge began an internal audit in September 2023

Contact

For any GDPR-related issues, contact the DPO or CEO (see Key Contacts).

Author	Date of Revision/Review	Comments
K. Cowie	10/03/2023	Major revisions
K. Kallmes	05/22/2023	Minor revisions
K. Cowie	05/21/2023	Minor revisions
K. Cowie	01/24/2022	Minor revisions
K. Holub	10/04/2023	Copy edits
K. Kallmes	11/19/2021	2021 version finalized and signed off

Return to Policies