NewNorm App
Privacy Policy

Last Updated: October 10, 2020

PLEASE READ THIS PRIVACY POLICY ("PRIVACY POLICY") CAREFULLY BEFORE YOU ("USER" OR "YOU") ACCESS, DOWNLOAD OR OTHERWISE USE THE NEWNORM MOBILE APPLICATION (THE "APP"), OUR PRODUCTS, DIGITAL CREDENTIAL-RELATED TECHNOLOGY AND ASSOCIATED SERVICES (SUCH AS DATA HOSTING SERVICES, THE IDENTITY-RELATED SERVICES AND OTHER INTERACTIONS BETWEEN YOU AND US, COLLECTIVELY, THE "SERVICES").

YOU ARE ACCESSING, DOWNLOADING OR OTHERWISE USING OUR APP AND SERVICES AT YOUR OWN WILL, AND IT INDICATES THAT YOU ACCEPT AND AGREE TO BE BOUND BY THIS PRIVACY POLICY IN FULL. IF YOU DO NOT ACCEPT THIS PRIVACY POLICY, OR IF IT IS NOT ABSOLUTELY VOLUNTARY, DO NOT ACCESS, DOWNLOAD OR OTHERWISE USE THE SERVICES. YOU ACKNOWLEDGE (A) THAT YOU HAVE READ AND UNDERSTOOD THIS PRIVACY POLICY; AND (B) THIS PRIVACY POLICY SHALL HAVE THE SAME FORCE AND EFFECT AS A SIGNED AGREEMENT.

This Privacy Policy is a summary of the manner and purposes for which we Process your Personal Data. It is designed to help you obtain information about our privacy regime, our practices and to help you understand your privacy choices when you use our App. Please note that our App offerings may vary by region. This Privacy Policy may be supplemented with additional notices depending on the region concerned. It applies to your Personal Data when you download and use our App, and does not apply to online websites or services that we do not own or control, including websites or services of other Users of our App.

We have defined some terms that we use throughout the Privacy Policy. You can find the meaning of a capitalized term in the Definition section.

Please contact us if you have questions about our privacy practices that are not addressed in this Privacy Policy.

1. Overview

ZAKA Group Ltd. is the developer of this App. Our digital identification technology, the App and Services are designed to provide a secure method for you to access and exchange identity-related information ("**Digital Credentials**") when dealing with various organizations without compromising your privacy.

This is achieved through ***Self-sovereign identity*** (SSI). For using our App and Services you will need to download the App, open it and read the Privacy Policy. Thereafter, we assign to you a Notification ID, which is a unique and anonymous ID number. The third-party services you choose to connect and agree to share your Notification ID with can then use your Notification ID to send notifications to your App. Your DID, or Decentralized Identifier, is a globally unique Digital Credential and resolvable via a ledger without requiring any centralized resolution authority. To maintain privacy each User can own multiple DIDs. The DID is generated uniquely for each service, stored in the App and not exposed to other parties in unencrypted form. All communications between services and the App are encrypted with the elliptic-curve ed22519 encryption system.

The App does not store any Personal Data in the Apps cloud, rather all personally identifiable information is stored on the device itself. It allows you to share your Personal Data with the third-party services that are listed in the App. Such a service may access, collect, use and store your Personal Data only upon providing you with an appropriate notification, upon receiving your explicit consent and according to their privacy policy which will be clearly made available to you before you share Personal Data with them.

With the exception of cases described in this Privacy Policy, we will neither access, collect or share any Personal Data while you are using the App, nor when you share your Personal Data with a third-party service in the App. In some rare instances described herein, if we access and use your Personal Data, we will notify you and ask for your permission each time. In all such instances we act as the Data Processor.

We utilize ***Zero-Knowledge Proofs*** (ZKPs) - ZK-SNARK ("zero-knowledge succinct non-interactive argument of knowledge"). This is a cryptographic technique, which allows you to share the information needed for a secure operation: you can provide a compact proof for requested credentials without revealing any other information. This will allow you, when appropriate, to share information without directly revealing your identity, nor relinquishing the security of your Personal Data. For a higher degree of ID verification, we offer an additional level of ID document and biometric authentication that is provided by third-parties whose privacy policies are clearly accessible when you use that service.

We use Hyperledger Indy as a backbone of our technology. This is an open source project under the Linux Foundation umbrella. These are tools, libraries and reusable components for providing digital identities rooted in blockchains or other distributed ledgers so that they are interoperable across administrative domains, applications, and any other silo. It uses open-source, distributed ledger technology with its own implementation of a PBFT-like public permissioned consensus protocol. (PBFT or Practical Byzantine Fault Tolerance, is the optimization of the Byzantine Fault Tolerance network ability of a network to unmistakably reach a consensus despite malicious nodes' attempts to propagate false data to other peers).

Effectively, this is Our NewNorm Ledger where we currently control the nodes. It is protected by strong, industry-standard cryptography. The result is a reliable, public source of truth which is not under a single entity's control, robust to system failure, resilient to hacking, and highly immune to subversion by hostile entities.

2. Information we collect and Process

Our NewNorm Ledger stores "Identity Records" - public data that may include public keys, service endpoints, credential schemas, and credential definitions – and nothing that would be Personal Data. Every Identity Record is associated with exactly one DID. Besides that, NewNorm Ledger stores a log of revoked credentials, none of which would contain Personal Data.

Our infrastructure maintains a list of Services in our cloud. Third-party providers maintain their own logs of on-boarded users, set and perform interactions and issue / receive verifiable credentials from the users by using NewNorm Platform which consists of backend (NewNorm Agent) and frontend (Service Dashboard). NewNorm Platform is delivered in the docker container and can be run on-premises or in any cloud service. NewNorm wraps the Indy SDK and enables you to have a unique digital SSI associated with them and stored in the App on your device.

The only thing that will be saved in the blockchain is the DIDs of services and data needed for checking issued credentials. The User decides with whom to enter into the peer-to-peer relationships and share credentials; or if a service wants to get credentials from a User, it shall make a request and the transaction will take place only if the User agrees thereto.

For the situation when a User wants to change his/her device, loss, etc. We may provide an optional backup service, which will allow the User to back-up the information in the App on the server of his/her choice. Our backup Service keeps the App encrypted by a key, which is known to the User and unknown to us or to the backup cloud service.

When providing Services to our clients, for example data hosting, we receive encoded data relating to their customers. When you contact us, we also may collect your name, phone number, email address and any other information you choose to provide to us.

When you chose to receive some of the Services provided directly by us, we may ask you for your Personal Data. In such instances you may share your Personal Data with us and only for the purposes described below. In such instance we Process your Personal Data. We do not extend usage of this Personal Data for serving advertising and we never sell or share your Personal Data.

3. Responsibility for Personal Data

In the course of providing some Services to our clients, we may Process Personal Data records of individuals who are our clients' customers or otherwise associated with our clients. In these circumstances, we act as Data Processor - we Process data on behalf of our client and on our client's instructions and the client is ultimately responsible for the Processing of the Personal Data of their customers. You will be asked to give your consent each time you share the Personal Data with a service and the service will not be able to see, access, store or use that Personal Data without your explicit consent. The service will also display and confirm your approval of their privacy policy prominently through the App.

We collect and Process Personal Data on our own behalf where the data is collected in connection with the administration of our business and Services. We may also collect Personal Data from Users of our technologies if we market and offer our technologies directly to them. In those circumstances, we are the entity which is responsible for the Processing of Personal Data. If you have any questions or concerns about our use of your Personal Data, please contact us at team@zaka.io and clearly mark the email as a privacy-related matter in the subject line.

4. How we use your Personal Data

The Personal Data obtained in the App or through the use of Services, and your other information may be used only for a couple of reasons that are justified under the applicable data protection laws.

- **To operate the App,** including to:
  - authenticate your access to the App;
  - communicate with you about the App;
  - create a connection between your Digital Credentials and a third-party account or platform
  - keep your Digital Credentials and information up to date.
- **To manage our business needs**, such as monitoring, analyzing, and improving the App performance and functionality. For example, we may analyze User behavior and perform research about the way you use our Services.
- **To comply with our obligations and to enforce the terms of our App,** including compliance with all applicable laws and regulations.
- **For our legitimate interests, including to:**
  - **enforce** the terms of our App;
  - **manage our everyday business needs**, such as monitoring, analyzing;
  - **manage risk, fraud and abuse of the App;**
  - **anonymize Personal Data** in order to provide aggregated statistical data to third parties, including other businesses and members of the public, about how, when, and why Users use our App.
- **With your consent, including to:**
  - To provide you with location-specific options, functionality or offers if you elect to share your Geolocation Information through the App. We will use this information to enhance the security of the App and provide you with location-based Services, such as advertising, search results, and other personalised (also called interest-based marketing) content.
  - To respond to your requests, for example to contact you about a question you submitted to our customer service team.

The nature of SSI allows multifunctional use of the App and Services. One of them is the App being used in **COVID-19 response, for example when you use the services of a third-party, such as an accredited and licensed medical lab, to issue or verify your COVID-19 test results**. In such instances, your communication with them is also peer-to-peer. You may be requested to share your Personal Data with the lab, or other medical service provider, who can then issue and or verify your test results to you as well as to a party whom you nominate to receive such results in a peer-to-peer way. Neither we nor our App will ever collect any medical information.

Our in-App disclosures accompany and immediately precede a request for your consent and, where necessary, an associated runtime permission. Neither us nor anyone else may access or collect any Personal Data until you consent to it. The App, Services and third-party services' requests for consent are clearly and unambiguously present in the consent dialogue for you to react on. We do not interpret you navigating away from the disclosure (including tapping away or pressing the back or Home button) as consent; and we do not use auto-dismissing or expiring messages as a means of obtaining your consent. You can withdraw your consent at any time and free of charge.

5. How do we work with other services and platforms?

For each Service and the third-party service, a User through the App generates a unique DID. You may use your DID and Notification ID to connect with a third-party account or platform. For the purposes of this

Privacy Policy, a “connection” with such a third-party is a connection you authorize or enable between yourself and an account not related to our App or Services. When you authorize such a connection, you and the third-party will exchange your Digital Credentials, Notification ID and other information including, as the case may be, your Personal Data and other information directly.

If you choose to create a connection, we may receive information from the third-party about the transaction and your use of the third-party’s service. For example, if you connect your Digital Credentials and Notification ID with a medical lab account, we will be aware of the connection but otherwise we will not know your identity or see your Personal Data if you choose to share them with such service provider.

Information that you share with a third-party based on the connection will be used and disclosed in accordance with the third-party’s privacy practices. Before authorizing any connection, you should review the privacy notice of any third-party that you want to authorize a connection with. This third-party may gain access to your Personal Data as part of the connection.

In addition, we may provide aggregated statistical data to third-parties, including other businesses and members of the public, about how, when, and why Users use our App and Services. This data will not personally identify you or provide information about your use of the App or Services.

6. Can Children Use Our App and Services?

The App and Services are not directed to children and/or persons under the age of majority in their respective jurisdictions and is intended for use by adults and/or persons at or over the age of majority only. We do not knowingly collect personal data from individuals under eighteen (18) years of age. If you are under the age of eighteen (18), please do not submit any information through the Services and do not provide your consent for the use of your data unless your parent or guardian has approved.

By letting your child use our App, you enable them to enjoy its features. By reading and confirming this Privacy Policy you accept that you will oversee and observe your child’s use of our App. Your child will be able to connect with Services, share Personal Data and receive Personal Data in return. Before your child may use the App, we must first obtain your consent to this Privacy Policy. In order to comply with General Data Protection Regulation (GDPR), the Children's Online Privacy Protection Act (COPPA) and similar laws in other jurisdictions, where applicable, that govern the online collection of data from children, we may take additional steps to help verify that the User granting permission for using our App is his or her parent or legal guardian. Accordingly, in these jurisdictions, you may be asked to verify your own credentials.

We will not collect, use or disclose any personal information from your child and the App will not collect such information without your verifiable parental consent unless a legal exception applies. Once you have reviewed this Privacy Policy, you will receive access to the App for your child. Your child will be able to use the App features, Services and third-party services.

We do not collect IP addresses. We may collect other information from the device that in some cases has been defined under applicable laws as Personal Data. For example, when your child is using our App, we may collect things like Device Information, cookies, the Geolocation Information and time zones in which the device is used. We also may collect information about your child’s activities and interactions on our websites, apps, products and Service.

We may use your child's information to communicate important notices and provide and improve our Service. We may also use his or her information for internal purposes such as auditing, data analysis and research. Your child will not receive advertising from us.

7. Changes to this Privacy Policy

We may revise this Privacy Policy from time to time to reflect changes to our busines, or Services, or applicable laws. The revised Privacy Policy will be effective as of the published effective date.

If the revised version includes a substantial change, we will provide you with 30 days prior notice by posting notice of the change on the "Policy Update" page of our website. We also may notify Users of the change using email or other means.

8. Contact Us/Communication

You may contact us, if you have general questions, concerns or complaints about this Privacy Policy and supplemental notices or the way in which we handle your information. We will respond to any of your inquiries by contacting you, if appropriate.

If you are not satisfied by the way in which we address your concerns, our Data Protection Officer can be contacted at team@zaka.io.

9. Definitions

App means our New Norm mobile apps and platforms, or other online properties through which we offer the Services, and which has posted or linked to this Privacy Policy.

Device Information means data that can be automatically collected from any device used to access the App or Services. Such information may include, but is not limited to, your device type; your device's network connections; your device's name; information about your device's web browser and internet connection you use to access the App or Services; Geolocation Information; information about apps downloaded to your device; and biometric data.

Digital Credentials means identity-related information. An identity "credential" (e.g. a passport) is comprised of one or more identity "attributes" (e.g. first name, last name, date of birth) and an attribute is a component of your identity. Digital credentials may refer to one or more credentials that are created, received, stored and shared through the App on your device.

Geolocation Information means information that identifies, with reasonable specificity, your location by using, for instance, longitude and latitude coordinates obtained through GPS or Wi-Fi or cell site triangulation.

Notification ID means the unique ID number that services you are connected with through the App can use to send notifications to your App on your device.

Personal Data means information that can be associated with an identified or directly or indirectly identifiable natural person. "Personal Data" can include, but is not limited to, name, postal address (including billing and shipping addresses), telephone number, email address, payment card number, other financial account information, account number, date of birth, and government-issued credentials (e.g.,

driver’s license number, national ID, passport number). It may also include any functionality or data regulated by dangerous or runtime permissions (including location, address-book, BSSID, BLE, photos, microphone, health sensors). The Personal Data does not include any data insofar as it is held, processed, disclosed or published in a form which cannot be linked to a living individual (such as anonymized data or aggregated data, which, in a given form, cannot directly or indirectly be used to identify you as an individual) ("Anonymized and Aggregated Data"). We reserve the right to generate Anonymized and Aggregated Data extracted out of any databases containing your personal data and to make use of any such Anonymized and Aggregated Data as we see fit (including publishing such data and sharing it with third parties).

Process means any method or way of handling Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, and consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data.

Services means any products, Identity-Related Services and other interactions between you and us, as well as any scenario when you use our content, features, technologies, or functions, and all related websites, applications and services offered to you by us through the App or otherwise.

Technical Usage Data means information we collect from your phone, computer or other device that you use to access the App or Services. Technical Usage Data tells us how you use the App and Services, such as what you have searched for and viewed on the App and the way you use our Services.

User (or “you”) means an individual who uses our App and the Services thereon.

ZAKA Group Ltd is the producer of the App and in this Privacy Policy is referred to as “we,” “us,” or “our,” depending on the context.