Huq Industries Limited
26-27 Bedford Square
London

The Danish Data Protection Agency
Carl Jacobsens Vej
35 2500 Valby
Denmark

Dear Mr Allan

I am writing in response to the inquiry you made to Huq on the 7th July 2021.

We would also like explain in a little more detail the basis of our business and our approach to the use of the data we work with.

Huq's business is to enable our customers to understand behavioural trends at scale. To ensure we are using data that has been collected in a GDPR compliant form we only use data that is collected through our direct relationships with mobile application developers (partners) with whom we maintain a direct contractual relationship. In turn all of Huq's customers are contractual obligated to make no attempts to reverse engineer any of the data in order to attempt to identify any individual.

All of our processes have been designed with advice from a UK based legal team experienced in GDPR. These processes have been audited and successfully passed inspection by both CNIL in France and the FTC in the US.

We sought to address each of your questions in line below and referenced where applicable accompanying documents which are separately attached.

1. **Provide a complete list of processing operations conducted by Huq Industries on data from Danish residents.**

   Categories of Personal Data

   Huq collects the following categories of personal data about consumers on the basis of consent:

   • Device details: Operating System, Date & time, Bundle ID, Device Model, Device Manufacturer, Carrier Code (Android only), Carrier Name, Sim Code, Country, and Locale

   • Location details including: Latitude, Longitude, Accuracy (GPS), SSID (network)

   Purposes of Data Processing

   Huq collects and processes personal data about consumers for the following purposes:

   • Building aggregated models of consumer behavior.

   Details of the processing steps that are applied are provided in the attached document: Huq_Privacy_Assesment.pdf

2. **This list shall contain the legal basis regarding every purpose.**

   In every case the basis for data processing is consent. We have a specific and small number of purposes. These are defined as "*the creation of anonymised reports, market research and trend analyses by Huq and its customers*"

3. **If the legal basis is original consent the wording and manner in which it is obtained**.

   Huq maintains a contractual relationship with each mobile app partner that supplies data to us. This contract requires that the partner obtains permission from the end user before the Huq SDK (the technical mechanism that enables data to be collected and passed to Huq) is activated.

Permission and explanation must be provided by our app partner in two forms. Firstly through an explicit consent window, see attached example (consent example.pdf) . Secondly the partner must also include the following clause in the mobile application terms and conditions: *"We collect the following information: Operating System, Date & time, Latitude, Longitude, Accuracy (GPS), SSID (network), BSSID (network), Bundle ID, Device Model, Device Manufacturer, Carrier Code (Android only), Carrier Name, Sim Code, Country, and Locale. In addition to helping us to measure the usage of our app this information is shared with Huq and its customers for their business purposes, which consist of the creation of anonymised reports, market research and trend analyses. Data shared with Huq does not contain information from which users can be identified by name and we will not provide additional information that enables Huq to identify you. You can find a full description of Huq and what it and its partners https://huq.io/data-partners do with the information collected via our app here https://huq.io/privacy-policy as well as details on how to request more information on the use of your data and your rights for editing or removing your data."*

Huq and our customers are seeking information on trends and we have no interest in profiling individual data subject and in consequence we do not seek consent for such profiling.

4. **Documentation and description on how, Huq industries verify that original consent is given**.

The Huq SDK is only activated when consent is granted by the end user as described above. Through the following clause in Huq's contract we test for compliance regarding consent and suitable terms and conditions wording: *"Huq reserves the right to reject Source Data where Huq has concerns about the Source Data, including (without limitation) the manner in which it is collected. No sums shall be paid to You by Huq in respect of such rejected Source Data. On Huq's reasonable request, You agree to provide copies of User consents or other evidence demonstrating Your compliance with these Terms of Service and/or any applicable laws relating to the collection and use of Source Data to Huq."*

Huq carries out automated testing of compliance to this clause on a monthly basis that ensures that suitable wording and reference to Huq's data processing activities are made in each app. Where permissions are missing on insufficient application partners are provided with an opportunity to rectify any issues or our contract with them is terminated.

5. **Any risk assessment considering the risk of rights and freedoms for natural persons with regards to the stipulated purposes and processing operations.**

In accordance with GDPR we maintain and update privacy impact assessment documentation. Our latest version is attached (Huq_Privacy_Assesment.pdf_

6. **It has been stated in the press that Huq Industries consider the data as anonymous. The Danish DPA kindly ask for an argumented position on the topic if this is in accordance with Huq Industries' viewpoint**

Huq offers a range of data products to its customers. The form of the data in these products is either pseudonymised, (in the case of our data feed product) or anonymised (in the case of our analytics tools). In addition, our customers are subject to strict rules regarding the use of the data that they obtain from us, and core amongst these rules is the requirement that our customers do not attempt to circumvent the pseudonymisation or anonymisation that we have carried out.

If you require any further information, then we will be happy to assist.

Yours Sincerely

Conrad Poulson

CEO, Huq Industries

e: hello@huq.io
s: https://huq.io
t: +44 (0) 203 808 8700

Privacy Impact Assessment: Huq Industries

1. Need and Scope

This PIA has been conducted in accordance with ICO guidelines and according to the ICO PIA template.

Huq uses human movement data collected via mobile devices to build models of consumer behavior in order to predict demand of products and services. The data is collected via an SDK incorporated into the mobile apps of Huq's partners ("mobile app partners").

Although all data is pseudonymized by the mobile app partners and Huq's processes, the following PIA has been carried out as a matter of good practice to ensure full measures have been taken by Huq to protect any potential areas of concern.

2. Processing

a) Key Steps

Huq uses an SDK distributed in the mobile applications of its partners. The process by which Huq collects data is as follows:

1. For each mobile app that incorporates Huq's SDK (the "SDK Apps"), Huq creates a universally unique identifier (UUID) using a one-way cryptographic hash for each device, as follows: the HuqID is an UUID created using the UUID5 method from the mobile device id (AndroidID or IdentifierForVendor ("IDFV")) together with a consistent namespace UUID to derive a consistent HuqID.
2. Once the HuqID has been generated, it is not possible to reverse engineer the process and return to the AndroidID or the IDFV from the HuqID.
3. The SDK collects the following information ("Data Points") by reference to the HuqID: Advertising ID (if permission received from end user), Operating System,* Datetime,* Latitude, Longitude, Accuracy (GPS), SSID (network), BSSID (network), Internal MAC address (network), Bundle ID, Device Model,* Device Manufacturer,* Carrier Code (Android only),* Carrier Name,* Sim Code,* Country, and Locale.* The actual Data Points collected depend on an app user's location and active use of the SDK App.
4. The Data Points are only collected when the app user (a) has location services enabled and (b) is actively using the app (unless the app user has permitted location services to run in the background) and (c) (as explained further below) has specifically consented to Huq's collection and use of the data, as required by Huq's terms with the partners who use the Huq SDK.
5. Huq cannot automatically request data collection via the SDK App and has no control over when and where the data is collected via the SDK App.

Huq's terms of service with the app developers require the app developers to actively and

specifically request permission from the app users to collect the Data Points and the individual has the right to withdraw this consent and switch-off the location services at any time.

b) Scope of the Processing

The raw data that Huq collects (as outlined in 2.a) undergoes a number of processing steps before it can be used by Huq and its customers. As well as deriving insight this processing ensures that Huq's raw data is never shared with 3rd parties.

Huq acknowledges that its collection and processing of location data (particularly patterns of movement) which is linked together under a random unique identifier may be sufficient enable an individual to be identified or singled out. This is why Huq requires users to specifically and actively consent to the use of location services by the SDK App and furthermore why all contracts with Huq's customers explicitly prohibit any attempts to identify named individuals through the use of Huq's data. The following clause is included in contracts with all customers of Huq's data and services:

"The Customer shall not, and shall not permit the Authorised Users or any other person to disaggregate, reverse-engineer or otherwise process the Data in such a manner that it becomes Personally Identifiable Data or otherwise decompile the Data, including by: combining or associating the Data with any other Personal Data (such as, but without limitation, first or last names, residential addresses, email addresses, telephone number or other contact details, or social security number, passport number or other unique descriptor) such that the Data becomes Personally Identifiable Data"

The Data Points collected from Huq SDKs are automatically passed directly to Huq without any additional assistance from Huq.

Processing involves the translation, using Huq proprietary technology, of the raw data into descriptions of the places and objects present in the locations that have been interacted with.

Descriptions of activity are then logged against the HuqID. It is this form of the data that Huq and its customers builds analysis on, however all data and analytics made available by Huq are subject to minimum thresholds and requirements to ensure customers are only granted access to aggregated data sets.

The processing applies to data collected globally by Huq without Geographic restriction when a user has permitted an SDK App to use and collect location data. No special category or criminal offence data is included.

c) Context of the Processing

Huq has no direct relationship with users of the SDK Apps.

Huq maintains, through a legal framework with its Mobile App partners, a requirement that individuals must both be informed of data collection and expressly and specifically authorize it, as is usual for the collection of location data.

Huq regularly audits Mobile App Partners to ensure compliance and retains the right to

reject/refuse data collected in contravention of this agreement.

Huq's relationship with individual data is one way in so much as Huq retains no return path through which to target, influence or contact individuals. This is because the one way hash used to create the HuqID cannot easily be hacked and even if it were, Huq would need additional information to enable it to link the Data Points to an identifiable individual.

Further data security is delivered using the following techniques:

- Raw data is stored separately from the processed form of the data.
- Pseudonymization of both the raw and processed data ensures that even in the event of a breach of Huq infrastructure the risk posed to an individual is minimal.
- All data is hosted within a secure cloud hosting environment.

d) Purpose of the Processing

The purpose of Huq's data processing is to understand human behaviour at scale through analysis of the patterns and trends that populations create. This analysis enables Huq's customers to make business decisions.

The wider benefits of this data can be applied to a number of elements of the physical environment. For example:

- Where a retailer should place a new store in order to best service the local population.
- How a transport provider should configure their route planning to optimize for travelers' needs.
- Determining the ideal location for new homes to best meet the needs of the market.

3. Stakeholder Consultation

We ensure regular dialogue between Huq's technical team through the CTO and CEO and Huq's privacy adviser. This dialogue ensures that any developments of Huq's data collection and processing are conducted in accordance with data protection guidelines. In return this dialogue ensures that any changes in regulation are highlighted to the right areas of the business.

We have close relationships with our customers and ensure that they are made aware of how we collect the Data Points, how they are stored and how they are converted to the data that they have access to.

We also monitor practices in our industry generally and ensure that we use appropriate technical and organizational measures to protect the Data Points.

4. Necessity and Proportionality of Huq Activities

Huq undertakes a series of technical and legal measures to ensure compliance.

Pseudonymization: Huq's business model is in no way related to targeting or influencing

specific individuals and therefore pseudonymization of all data collected is possible and performed. Huq applies methods at both collection and processing layers to achieve this.

Legal: Huq requires any customers of its service to warrant that no attempts will be made to reverse engineer any Huq derived data.

Testing: Huq conducts and documents regular testing of its data to ensure reverse engineering to any personally identifiable individual is not feasible.

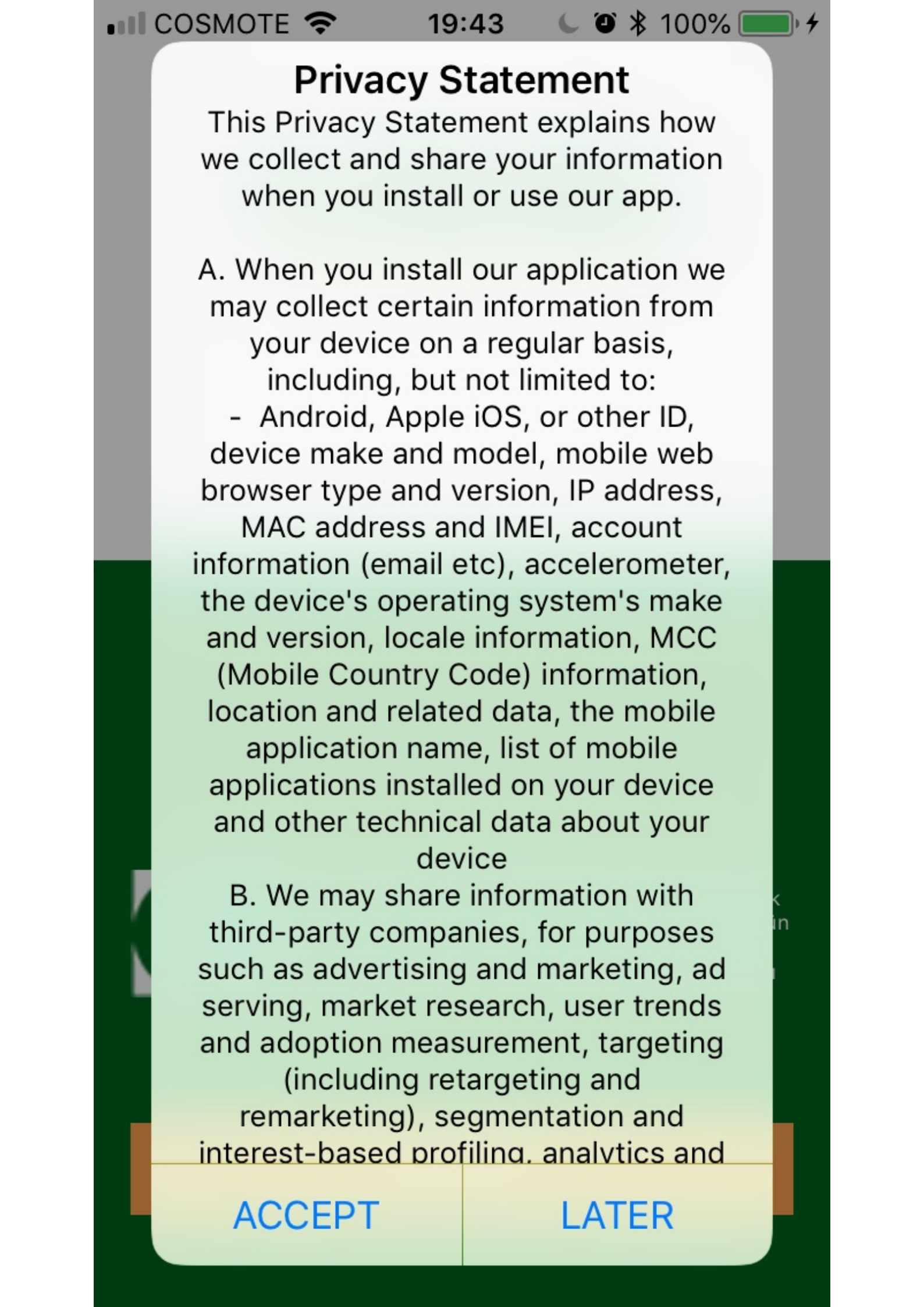
All data processing is managed directly by Huq with no dependencies on external parties.

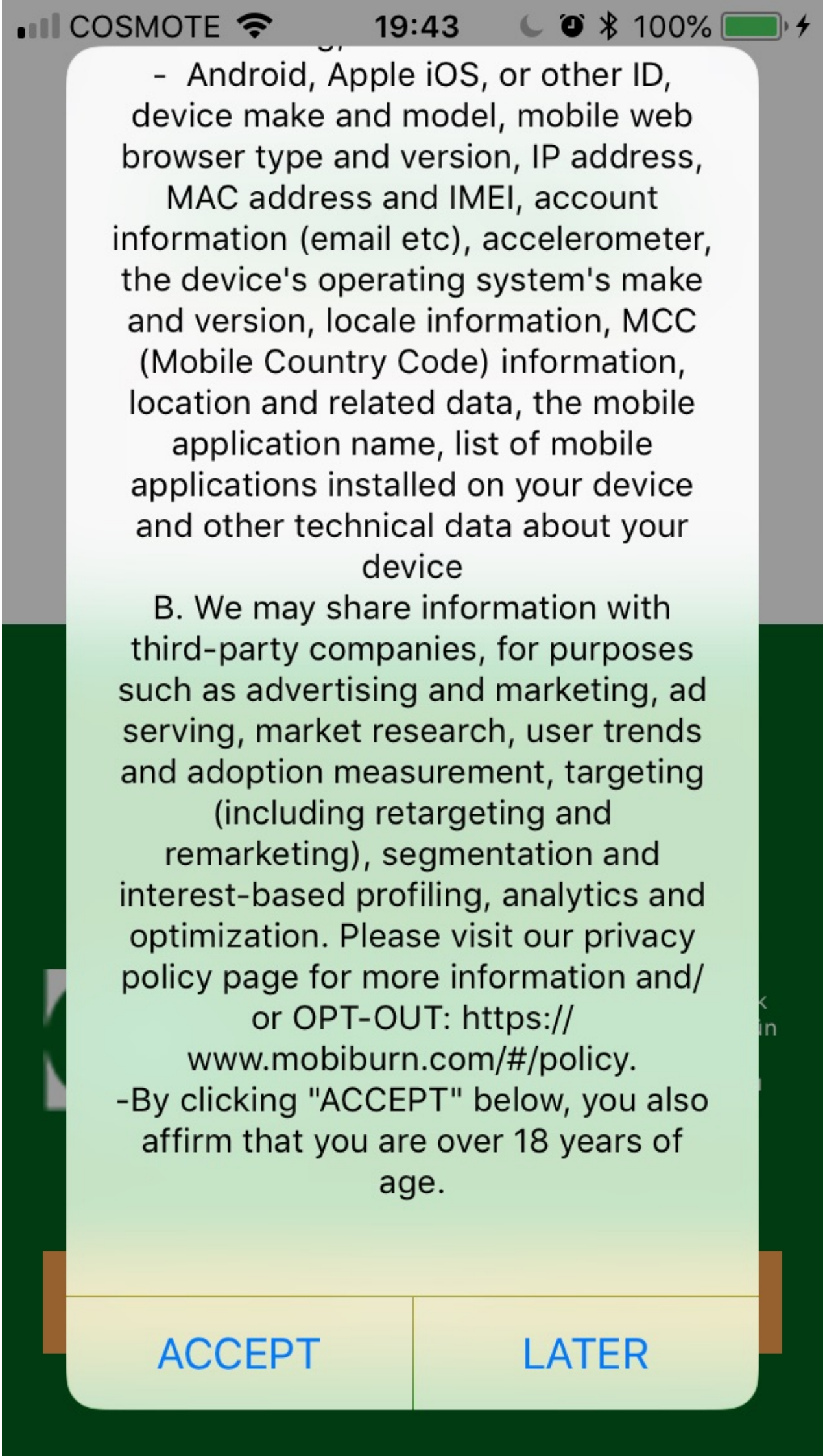
5. Risk Identification and Assessment

Source of risk and nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Overall risk
The key risk to assess is the possibility of an individual and their behavior being identified from the Huq data.	Remote	Significant	Low

6. Risk Reduction Measures

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk
Individual identification	Clustering of data to make individual identification impossible	Eliminated	Low
Individual identification	Obfuscation of accuracy readings to make precise identification unfeasible.	Reduced	Low


COSMOTE
19:43
100%
Privacy Statement
This Privacy Statement explains how we collect and share your information when you install or use our app.
A. When you install our application we may collect certain information from your device on a regular basis, including, but not limited to:
- Android, Apple iOS, or other ID, device make and model, mobile web browser type and version, IP address, MAC address and IMEI, account information (email etc), accelerometer, the device's operating system's make and version, locale information, MCC (Mobile Country Code) information, location and related data, the mobile application name, list of mobile applications installed on your device and other technical data about your device
B. We may share information with third-party companies, for purposes such as advertising and marketing, ad serving, market research, user trends and adoption measurement, targeting (including retargeting and remarketing), segmentation and interest-based profiling, analytics and
ACCEPT
LATER


COSMOTE
19:43
100%
- Android, Apple iOS, or other ID, device make and model, mobile web browser type and version, IP address, MAC address and IMEI, account information (email etc), accelerometer, the device's operating system's make and version, locale information, MCC (Mobile Country Code) information, location and related data, the mobile application name, list of mobile applications installed on your device and other technical data about your device
B. We may share information with third-party companies, for purposes such as advertising and marketing, ad serving, market research, user trends and adoption measurement, targeting (including retargeting and remarketing), segmentation and interest-based profiling, analytics and optimization. Please visit our privacy policy page for more information and/ or OPT-OUT: https:// www.mobiburn.com/#/policy.
-By clicking "ACCEPT" below, you also affirm that you are over 18 years of age.
ACCEPT
LATER