



# Privacy Charter

Prepared by Tutela Technologies Ltd.

Hunter Macdonald, CEO  
Devan McCannel, Mobile Partnerships Manager, and  
Anthony Kroeker, VP Engineering Systems & Data Protection Officer

Tutela's privacy controls and practices have been reviewed, on the basis of a Privacy Assessment, by PricewaterhouseCoopers



Last updated: December 4, 2020

**TUTELA** 

# Tutela Privacy Charter

Tutela works with telecoms companies globally to help them understand and improve network speeds and network coverage for consumers like you. We help them build better networks in the areas that need it most. Tutela takes great pride in providing a public good service that is an improvement on alternative telecom solutions that are often more expensive with greater carbon emissions.

As a company whose livelihood depends on data and its proper treatment, Tutela takes data privacy and security very seriously. As such we have taken steps to go well beyond basic privacy and data protection requirements.

Tutela collects many statistics and measurements, but we do not collect any personal information that is directly attributable to individuals. We do not collect any persistent device identifiers from consumer devices. Our products and services do not require user identification. We take appropriate administrative, commercial, and technical measures to ensure that our datasets are not used by Tutela, our partners, or our customers, to identify individuals.

## Why we collect data.

Tutela is a world leader in improving communications networks based on users' perspective of performance. We collect data so that we can help communications service providers, network equipment manufacturers, and other third parties within the telecom ecosystems better benchmark, understand, and improve consumer experiences on networks. Our data is only used within the telecoms ecosystem and only for the purpose of understanding, communicating, and optimizing network performance.

As an example, we often use data to identify areas where there is poor WiFi or cellular signal so that wireless carriers can fix their network issues and improve performance for their subscribers.

## How we collect data.

Collecting data from millions of devices is a significant challenge. Our research showed that users did not want to install more applications on their devices to collect data, but were happy to provide pseudo-anonymous ("pseudonymous") data if it helped to reduce advertisements, improve mobile signals, and if it did not affect their experience or device performance.

With the appropriate user permissions, our software runs in the background of popular mobile apps and games to collect data. This helps us to collect as much useful data as possible, without requiring the user to download another application. In many cases, this also means that the mobile apps can display fewer advertisements to users because mobile applications are paid to partner with us and for their contributions to improving world-wide connectivity.

All of our mobile application and games partners are required to provide disclosures and permission requests to their users to enable pseudonymous data collection, and abide by all applicable global privacy legislation. Tutela regularly audits our partners to ensure compliance.

## What data we collect.

All information we collect is kept pseudonymous or anonymous at all times. Pseudonymous means that separate data sets, not held or processed by Tutela, would be required to identify individuals. Tutela ensures that this attribution is both difficult and strictly prohibited through licensing provisions.

Tutela's application partners configure the Tutela data collection library based on their data collection user permissions, user disclosures, and data policy. The information actually collected by Tutela may differ on a case-by-case basis based on this partner configuration. This information includes:

Category	Typical Use
<b>Device &amp; Environment Characteristics</b> including Device Make, Model, OS Version, Screen Resolution, Lux	Wireless device details are required to identify if specific network issues are limited to a device type or indoor/outdoor environments.
<b>Geolocation</b> information about the location of the device, including latitude and longitude	Required to aggregate and plot network performance on a map to convey network coverage in a given area.
<b>Connection Details</b> information about the network connection, including Service Provider, Cell Tower ID, BSSID (if a WiFi connection), non-identifying IP addresses	Used to separate data and results by operator and compare their performance, and congestion, to help with competitive analysis. Traceroute ping tests indicate the IP Addresses of commonly accessed network elements (ex: servers, gateways, etc.) but not the device (or router's) public IP.
<b>Connection Quality</b> including passive tests (e.g. signal strength) and also active tests (e.g. download speed)	Used to evaluate the performance of wireless networks.

<b>Video and media service performance</b> including Playback Errors, Buffering Interval, Latency Response time	Video tests are a different form of network test performed by Tutela intended to estimate video performance. Test videos are streamed in the background. For clarification, Tutela does not monitor consumer video traffic.
<b>Daily Session Tag</b>	The Daily Session Tag is a randomly assigned and temporary session identifier. It is used to determine, for discrete 24-hour periods, the breadth and statistical reliability of our wireless insights. (More information below).
<b>State of Test Application</b>	The state of this application during a network test (e.g. "in use") may be collected for data validation purposes. Tutela never sees or records any content viewed by users.

Every end user agrees and opts in to sharing this data with Tutela by accepting their mobile application's permissions and privacy policy. We require that all appropriate consents are granted. Furthermore, our licensing mandates that our application partners provide complete disclosures to end users listing what is collected and how it is used. We audit our application partners regularly to ensure that these requirements are being satisfied.

## Where we collect data.

Tutela collects data wherever there is an opportunity to improve wireless networks. We may implement more strict collection and storage practices based on geography to comply with region specific privacy and data protection requirements.

## We prevent user identification.

We do not collect any sensitive personal information from users. We never collect name, email address, phone number, social media ID, contact list, or anything else which directly identifies individuals.

Additionally, we do not collect or store a persistent internal device ID. Each mobile application install sending us data is assigned a random identification code generated by our software (called a "Daily Session Tag"), which is used to create daily aggregate metrics and assess the statistical significance of our wireless insights. Our Daily Session Tag represents measurement sessions and resets every 24 hours to a new random number and cannot be reversed to arrive at a persistent ID.

## We transmit and store data secure from malicious attacks.

We use the latest data security methods and premium data centers to ensure data is held securely. Our data is stored in databases encrypted using 256 bit AES encryption and access requires 2-factor authentication.

When data is transferred from mobile devices to our database, we use 256-bit encryption. We monitor the access to our databases carefully to identify any breach of security.

We collect and store only the data we need for our business. No raw data is stored by Tutela for more than 18 months.

## We are transparent about why we collect data and how we will use it.

Our data is only used within the telecom ecosystem to understand, communicate, and optimize network performance. For example, we use data to improve wireless networks, identify aggregate trends in device and network utilization patterns, understand the network-based drivers of subscriber churn and acquisition, and design effective network performance communication campaigns.

Tutela's documentation, available at <https://insights.tutela.com> publicly discloses all data we collect, how we collect it, and how it is used. This information disclosure is available to everyone, including our competitors, in the interest of full transparency.

For more detail on the nature of our relationship with mobile applications, including their requirements and our provided documentation, please visit <https://www.tutela.com/app-developers>.

## We only share data with trusted companies.

Our data is only shared with companies within the telecom ecosystem that agree to our strict privacy and data handling terms, or adhere to their own equivalent privacy terms.



Tutela may share pseudonymous data collected from users of applications running Tutela's software, including geolocation data, network element identifiers, the Daily Session Tag, and internet or other electronic network activity information:

- a. With our customers: Tutela's customers are generally major communications service providers. You can learn more about our common solutions at <https://www.tutela.com/solutions>.
- b. With our employees: On a need-to-know basis Tutela allows employees to access data so that we might service our customers or develop products.
- c. With our service providers: For example, for website and data hosting, or hiring auditors to review and ensure our privacy policies and practices meet the highest standards.
- d. With service providers to our customers: Our customers may contract with companies to help them derive additional value from Tutela's products and data.
- e. With our subsidiaries and affiliates: In 2019 Tutela was acquired by Comlinkdata. Together we are proud to bring together complementary data on consumer experience, network performance, and subscriber behaviour. As a merged company we help the telecoms industry to understand and execute on opportunities to better meet the needs and wants of consumers. <https://www.tutela.com/tutela-and-comlinkdata-announcement>
- f. With public authorities, such as law enforcement: If we are legally required to do so or if we need to protect our rights or the rights of third parties.

## Data collection will not negatively impact our users.

Providing data to us does not have any negative impact on users or their devices. Data we collect cannot be used to disadvantage our users. Quite the opposite; our data is typically used to improve networks and ensure a better experience for users.

The impact to the device battery and CPU is designed and tested to be so small that it cannot be noticed by the average user (less than 1%). For our mobile application and game partners, the additional file size is less than 1 MB. Tutela does download and upload files to test network performance which may count against user data quotas. We work with our app partners to ensure that this doesn't exceed levels which are acceptable or generally expected from their app.

## Our mobile app partners are anonymous.

Our customers and partners cannot use our data to identify the mobile applications or publishers that our data has been received from. We collect data from hundreds of different mobile applications, and our reports, data, and documentation do not reveal which mobile applications the source data was collected from. We do not publicly disclose our application partners without their permission.

## Children's Privacy.

Our services are not intended for children under the age of 16, and we do not knowingly collect information from children under the age of 16. We require that our mobile application partners agree to not include Tutela's software in applications that are targeted to children and regularly audit our partners' applications for violations.

## National and State Data Protection Acts.

Tutela and its partners take appropriate measures to ensure compliance with data protection legislation in the countries where they offer their services.

## We make it clear how you can opt out.

Users are made aware that they are participating in the collection of Tutela's pseudo-anonymous statistics prior to downloading and then using an application. In all cases this is explicit and disclosed in the privacy policy that is available on the download pages of participating applications. We also make use of the standard iOS/Android permission requests for data such as location, and in some cases work with our partners to design custom in-app pop-ups which provide even more in-app detail. The procedure for later opting out is generally found in the application's privacy policy, terms of service, and/or settings menu. Additional opt-out instructions are detailed below.

Note: In exceptional cases we allow individual users to opt-in to provide additional data to Tutela for advanced service troubleshooting. This involves a secondary in-app pop-up consent request beyond basic permission requests. Data includes things such as; when, where, and why phone calls fail; or providing IP address information. These special troubleshooting cases may include data types which are additional to those listed above - which describe the capabilities of our standard configurations available to all mobile applications.

## Your rights as a data subject.

GDPR and other forms of legislation provide data subjects with certain legal rights in respect of their personal data.

a. **Right to Access:** the right to obtain from the controller confirmation as to whether or not personal data concerning the data subject are being processed. Please note that Mobile Advertising IDs are not collected from devices in GDPR participating countries.

b. **Right to Rectification:** the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

c. **Right to Erasure:** the right to obtain from the controller the erasure of personal data concerning him or her without undue delay.

d. **Right to Restriction of Processing:** the right to obtain from the controller restriction of processing where certain conditions are satisfied.

e. **Right to Data Portability:** the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

e. **Right to Object:** the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her.

f. **Right to Lodge Complaints:** you have the right to lodge a complaint with a supervisory authority or other regulatory agency if you believe that we have violated any of the rights concerning personal data about you. We encourage you to first reach out to us at [data.protection.officer@tutela.com](mailto:data.protection.officer@tutela.com) so we have an opportunity to address your concerns directly before you do so.

The above legal rights are subject to various conditions and exceptions. We take steps to help ensure that you are able to exercise your rights. However, the pseudonymous nature of our data may mean that it is impractical to satisfy certain requests as it is materially difficult or not possible to associate data with your identity. To make a request in accordance with the GDPR, please submit your request via the Data Privacy Request web form available at [tutela.com/opt-out](https://tutela.com/opt-out), or send an email to [data.protection.officer@tutela.com](mailto:data.protection.officer@tutela.com) with "GDPR Privacy" in the subject line.



## Your rights as a California resident.

The California Consumer Privacy Act (CCPA) provides residents of California with certain legal rights in respect of their personal information.

a. **The Right to Know:** you have the right to request that we disclose the categories of personal information we have collected, sold, and/or disclosed for a business purpose about you; the categories of sources from which we have collected your personal information; the business or commercial purpose for collecting or selling your personal information; the specific pieces of personal information we have collected about you; and the categories of third parties to whom your personal information was sold. Tutela is not required to respond to requests to know more than twice in a 12-month period.

You may submit a request to know via the Data Privacy Request web form available at [tutela.com/opt-out](https://tutela.com/opt-out), or by calling toll-free at +1 (855) 6-TUTELA (ext. 5). We will acknowledge the receipt of your request within ten (10) business days of receipt. Subject to our ability to verify your identity, we will respond to your request within forty-five (45) calendar days of receipt. In order to protect your privacy and the security of your personal information we typically verify your request by requesting additional identifying information relating to you and/or your mobile device such as the mobile advertising ID. If we deny your request for any reason we will explain why.

With respect to requests for specific pieces of personal information, we have determined that there is a substantial safety and security risk to a person in disclosing the geolocation of a device to another person who (i) is not the actual user of a mobile device with which geolocation data is associated, but (ii) has an interest, whether lawful or unlawful, in gaining access to geolocation data associated with a device and the movement patterns of the actual user of the device. Given this risk, and (i) since we do not seek to determine the actual identity of persons that use mobile devices for our business purposes; (ii) we do not collect identifiers such as names, addresses, cellular/mobile phone numbers, or persistent device identifiers; and (iii) because we do not wish to collect extensive additional personal information for verification purposes, we have concluded that we currently have no reasonable method to verify the identity of the person making a request for specific personal information to a reasonably high degree of certainty. Consequently, we will treat requests to know specific pieces of personal information as requests to know categories of personal information. We will re-evaluate this determination on a yearly basis.

Within the past 12 months Tutela has sold or shared the following categories of personal information: (1) Geolocation, (2) Identifiers, and (3) Internet or other electronic network activity information.

Within the past 12 months Tutela has disclosed for a business purpose the following categories of personal information: (1) Geolocation, (2) Identifiers, and (3) Internet or other electronic network activity information.

**b. The Right to Delete:** you have the right to request that we delete any personal information about you that we have collected from you.

You may submit a request to delete via the Data Privacy Request web form available at [tutela.com/opt-out](https://tutela.com/opt-out), or by emailing [data.protection.officer@tutela.com](mailto:data.protection.officer@tutela.com) with "CCPA Privacy" in the subject line. We will acknowledge the receipt of your request within ten (10) business days of receipt. Subject to our ability to verify your identity, we will respond to your request within forty-five (45) calendar days of receipt. In order to protect your privacy and the security of your personal information we typically verify your request by requesting additional identifying information relating to you and/or your mobile device such as the mobile advertising ID. If we deny your request for any reason we will explain why.

**c. The Right to Opt-out:** you have the right, at any time, to direct us to not to sell your personal information to third parties.

You may submit an opt-out request by following the steps outlined in the Opt-out Options section of this Privacy Charter below, via the Data Privacy Request web form available at [tutela.com/opt-out](https://tutela.com/opt-out), or by emailing [data.protection.officer@tutela.com](mailto:data.protection.officer@tutela.com) with "CCPA Privacy" in the subject line. Subject to our ability to verify your request, we will respond to your request within fifteen (15) business days of receipt.

**d. The Right to Non-Discrimination:** a business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under the CCPA.

**e. Authorized Agents:** Authorized agents may make requests under the CCPA on a consumer's behalf in compliance with the [CCPA Regulations](#) by following the same guidelines outlined above.

The above legal rights are subject to various conditions and exceptions. We take steps to help ensure that you are able to exercise your rights. However, the pseudo-anonymous nature of our data may mean that we are not able to sufficiently verify the association between our data and individual consumers.

## Tutela Opt-out.

Tutela is unable to collect data without having the end user opt in by accepting application permissions and any other consent configured by our application partners. Procedures are provided to support individuals to opt out at any time, as outlined below and at <https://tutela.com/opt-out>.

## Opt-out options.

1. End users may review the privacy policy(s) and/or in-app settings of an application or a group of applications containing Tutela's software for application-specific opt-out instructions.
2. End users may at their option restrict an application or a group of applications from collecting location data. No data will be collected by Tutela if location permission is not enabled for that app. Please note that if you do deny or revoke location permissions for an application, certain functionalities of the app that rely on location data to function may be affected.

For Location Turn-Off instructions on Android mobile devices visit <https://support.google.com/accounts/answer/6179507>, and for Location Turn-Off instructions on iOS mobile devices visit <https://support.apple.com/en-us/HT203033>.

3. End users may at their option uninstall and stop using applications which have requested data permissions. Tutela's software will be uninstalled along with our partner application.
4. In accordance with the CCPA, if you are a California resident or authorized agent you may submit an opt-out request via the Data Privacy Request web form available at [tutela.com/opt-out](https://tutela.com/opt-out), or by emailing [data.protection.officer@tutela.com](mailto:data.protection.officer@tutela.com) with "CCPA Privacy" in the subject line.
5. If you qualify as a data subject under GDPR you may submit your request via the Data Privacy Request web form available at [tutela.com/opt-out](https://tutela.com/opt-out), or by emailing [data.protection.officer@tutela.com](mailto:data.protection.officer@tutela.com) with "GDPR Privacy" in the subject line. note

Please note Tutela has taken extensive steps to make identification in our data difficult. These measures, which are in the interest of safeguarding the privacy of our users, similarly restricts some forms of information, opt-out, and deletion requests because it has been made purposely difficult to identify you or your data in our datasets.

## Notes on this Privacy Charter.

From time to time we may update this Privacy Charter. You can tell when changes have been made by referring to the "Last updated" date at the top. Please review this Privacy Charter regularly to ensure that you are aware of any changes.

This document does not encompass or detail Tutela's handling of internal employee or customer data. Tutela's employees and customers may provide additional personal information such as names, email addresses, and phone numbers through the regular course of business and Tutela's non-public facing policies, which are available to those groups, govern the handling of that data.

## Data Protection Officer.

Please contact Tutela's Data Protection Officer with any questions or for GDPR, CCPA, or other privacy legislation supported requests. We ask that you limit these messages to only contain information about you that you are willing to share with Tutela. Responses pertaining to data from your mobile may be limited due to the pseudo-anonymous nature of our data set and the identification limitations that places on Tutela.

[data.protection.officer@tutela.com](mailto:data.protection.officer@tutela.com)