Crowd Connected's Colocator Technology and GDPR

This document sets out how our Colocator location intelligence software collects, processes and stores data for the provision of location-based services to our clients in the context of the General Data Protection Regulation ("GDPR"), the new European privacy law which comes into effect on 25 May 2018. Your attention is also drawn to the notice at the foot of this document.

What data is collected, processed and stored, and does this data constitute 'personal data' under GDPR?

The data collected by our Colocator platform consists of unique app install identifiers, geolocation data, WiFi and Bluetooth signal strengths, plus additional metadata sourced from the device's operating system which may include inertial data, hardware and operating system details, device identifier and battery strength (collectively "Input Data").

Colocator Input Data is sourced from a person's mobile phone, via our code embedded into an app downloaded onto the device. So Input Data is every message sent by a mobile device to our cloud-based back-end platform.

We take the Input Data and process it on our servers into trajectory histories consisting of unique device identifiers (our own and app-provided) and geolocation data ("Output Data"). We store both the Output Data and the original Input Data in cloud storage. We contract Amazon Web Services for cloud-based processing and storage.

All the data, whether Input Data or Output Data has no directly identifying data, and is therefore pseudonymous by design from source – without any additional transformational steps needing to be applied to effect pseudonymisation.

While location data is not defined by GDPR, it is specifically cited as an example which *may* constitute personal data because it *could* be used, when combined with other data, to determine where an individual lives and/or works, find out social, religious or cultural identity, and personally identify them. Similarly non-location data such as a unique device identifier might also be combined with other data to identify someone.

Personal data is defined by GDPR as any information relating to an identified or identifiable natural person.

Arguably there are instances where the data we collect, process and store does *not* constitute personal data as defined under GDPR (for example, because the stream of location data points associated with a unique app install identifier is limited by time or location, and therefore it would

be extremely difficult to identify the person using additional information in combination with Colocator data).

Whether or not data collected, processed and stored by Colocator does constitute personal data as defined under GDPR is, in practice, a complex question dependent on the specific circumstances pertaining to the time/place/frequency/granularity of data collection. Furthermore, exactly how much effort might be required to identify the owner of the device from the data is open to debate.

Our approach: treat all Colocator data as personal data

We believe the most prudent, pragmatic and indeed the best practice approach is to treat all Colocator data collected from deployments of our technology in the European Union as being subject to the relevant GDPR regulations (as enacted into national law).

We ensure we are fully GDPR compliant to the extent required under appropriate national law, with applicable policies, procedures and systems in place and documented. Further detail on our compliance is provided in the data processing addendum to our standard Colocator services terms and conditions as well as in our data security documentation.

We only source Colocator data with explicit consent

We work closely with app developers who are responsible for putting in place applicable user interfaces within the app for obtaining prior, informed, explicit, unambiguous, affirmative consent from the end user, the data subject (i.e. the person using the mobile phone). It is the app developer's responsibility to activate our code library only once such consent has been obtained, and only then do we collect, process and store data. This consent must be purpose-specific. If such consent is subsequently rescinded, it is the app developer's responsibility to de-activate our code library.

Our data collection methodology is therefore fundamentally different from, for example, techniques commonly known as WiFi 'sniffing' which passively collect location data from devices without necessarily obtaining the end user's explicit consent. Where we use signals emitted by a device to locate it, we do so only via the app, and therefore always with the explicit consent of the owner of the device that is being located.

As we have previously highlighted, the way Colocator collects, processes and stores data is pseudonymous by design, i.e. such that the data does not directly identify an individual without the use of additional information.

Consequently, while that means our data services are subject to the requirements of GDPR, we benefit from relaxations of certain provisions, in particular with respect to data breach

notification requirements, exemption from the need to comply with data subject access, correction, erasure and data portability requests, and greater flexibility to conduct further data processing without data subject consent.

Data processing, storage and security

Colocator Input Data is transmitted in encrypted form to our servers hosted on Amazon AWS, where it is processed. Both the Input Data and the Output Data are then transmitted to an AWS S3 cloud storage service where they are stored. The physical location of these AWS services is agreed with our clients.

AWS offers, and Crowd Connected benefits from, a wide range of services and features designed to meet various requirements of GDPR, including services for access controls, monitoring and logging. AWS boasts industry-leading security which provides the foundation for internationally recognized certifications and accreditations, including ISO 27017 for cloud security and ISO 27018 for cloud privacy.

AWS has confirmed that “AWS services comply with GDPR”:
see: https://aws.amazon.com/compliance/gdpr-center/.

Crowd Connected as a data processor

Almost without exception, in relation to GDPR Crowd Connected acts as a ‘data processor’ – i.e. processing data on behalf of a ‘data controller’. It is the data controller (i.e. most frequently our client, who will also have commissioned the mobile app into which our Colocator code library is integrated) which determines the purposes for which the data is processed by us. We always process Colocator data in accordance with the controller’s instructions and, in any event, under a binding contract.

Notice

Crowd Connected’s customers are responsible for making their own independent assessment of the information in this document and any use of Crowd Connected’s Colocator products or services, which are provided “as is” without warranty of any kind, whether express or implied. This document does not form part of, nor does it modify, any agreement between Crowd Connected and our customers.

v1.4, updated May 2019