Telia

IOT + DATA PROTECTION

An introduction

Personal data and data protection can be tricky. We have made this introduction to share our view on how GDPR and other regulations apply to Telia's IoT services. We hope that you find it useful.

DATA TYPES

Operating our IoT services means that we process various types of data. One of the categories is ***Traffic Data***. Traffic Data is the data generated as signals flow through our mobile networks. Basically, it is information on data packages, answering questions like when data was transmitted, from which location to which receiver, and what was the size of the data package. This type of data is used *e.g.* to monitor and improve our services, determine load levels in the network and for billing purposes.

We also handle ***Content Data***, meaning data produced by the customer's devices that are connected through our IoT services. Content Data is sometimes regarded as Personal Data, but not always. By way of example, information generated by a connected vehicle reporting its position in real time is Content Data. But this location information is typically also considered Personal Data since it can be used to identify an individual, the driver, for as long as someone has knowledge connecting the specific vehicle with the driver (*e.g.* through a register kept by the customer). On the contrary, Content Data made up by weather information collected from sensors in a connected weather station is very unlikely to include Personal Data, as there is typically no link to an individual. Content Data is always owned by the customer.

We also process ***Administrative Data***, being used for the purposes of *e.g.* customer personnel logging into a service portal and contact details belonging to service users. Handling this type of data is a biproduct of the interactions between Telia and service users, bringing our IoT services to our customers.

PERSONAL DATA?

So, what is ***Personal Data***? Well, this is not determined by us, but by the EU's General Data Protection Regulation (GDPR). The definition of Personal Data is very wide and captures any data or information that can be linked to an individual, directly or indirectly. The tricky part is that collective (indirect) knowledge is applied. This means for example that if two parties (in this case, Telia and the customer) have shared access to data which links to an individual when put together, even if the parties do not have direct access to each other's data, such data is regarded as Personal Data. Simply put; regardless if we look at Traffic, Content or Administrative Data, such data is also Personal Data *if there is a direct or indirect link between the data and an individual*.

DATA PROTECTION – ROLES

Handling Personal Data is subject to regulation, most recently through the GDPR. But the GDPR of course contains more than a definition of Personal Data; it also includes concepts of different roles when processing Personal Data.

Being a ***Controller*** means that you are the one ultimately responsible for the processing of Personal Data for a specific purpose. For each purpose, the Data Controller must have a legal ground for the processing in order for it to be GDPR compliant.

A ***Processor*** is an entity tasked with assisting the Controller with its processing of Personal Data, and that task *must be documented in a data processing agreement* (governing all details of the processing of Personal Data). A Processor may only process Personal Data in accordance with the instructions from the Controller. It is not allowed to process the Personal Data for its own purposes and always relies on the Controller's legal ground for all Personal Data processing activities.

ROLES IN TELIA'S IOT SERVICES

Now it is time to look at data in Telia's IoT services and what type of role Telia and its customers take when Personal Data is processed in the service (assuming here that all types of data mentioned below also constitutes Personal Data).

Traffic Data and Administrative Data
To the extent Traffic Data also constitutes Personal Data and is processed for the purpose of delivering a Telia service, Telia regards itself as Controller of such Personal Data. The same applies for Administrative Data.

Content Data
For Content Data (which is also Personal Data) the picture is a bit more complex.

In its basic form, Telia's IoT service is pure connectivity (making sure that data is being transmitted from point A to point B).

When providing this telecom service, Telia is subject to regulation and specific legal obligations to ensure that the service is efficient, safe and secure (for instance, there are legal requirements with respect to encryption of transmission); Telia may process all previously mentioned categories of data for the sole *purpose of providing the connectivity service* to its customer. And when processing Content Data for that specific purpose, Telia is the Controller. Consequently, Telia and its customers do not need to enter into data processing agreements as long as the connectivity service is the only service provided by Telia (assuming that Telia does not process Personal Data for any other purpose than providing the connectivity service).

However, the situation is different if the customer is using add-on services available in Telia's IoT platform, or if Telia is otherwise tasked by the customer to process Content Data for another purpose.

This is the case for example when Telia is supplying the customer with services regarding data storage, data analytics or data visualisation. In these cases, Telia is processing Content Data on behalf of the customer for a purpose beyond delivering data from point A to point B. Consequently, the customer is a Controller and Telia is a Processor, and *Telia and the customer must have a data processing agreement in place*.
A telecom specific privacy law is applicable for Telia and other telcos providing telecom services. That law is currently the EU's Electronic Privacy Directive (ePD). ePD is presently being reviewed and we expect a new law to be adopted Q4 2021/Q1 2022, where IoT services might be regulated separately.
The current implication of ePD on IoT services is that even when Traffic Data or Content Data is not Personal Data, it is still subject to specific confidentiality obligations and restrictions in terms of certain types of processing. But that is for Telia to comply with.

FINAL WORDS ON GDPR

Telia's IoT services are set up to be GDPR and ePD compliant (including with respect to security surrounding the IoT services), meaning that the mere fact that a customer is using the services does not mean that there is a breach against GDPR. But it is always the responsibility of the customer to make sure that Content Data which is also Personal Data is handled in a way that is compliant with applicable laws (including requirements such as data mapping, securing that all data processing lives up to GDPR's requirements and that data subject's rights are observed). Then again, these requirements apply for the customer deploying IoT solutions, regardless if Telia is the provider of these type of services or not.

We hope that this introduction helped in gaining a basic understanding of how Personal Data is handled in our IoT services.

Notes

A telecom specific privacy law is applicable for Telia and other telcos providing telecom services. That law is currently the EU's Electronic Privacy Directive (ePD). ePD is presently being reviewed and we expect a new law to be adopted Q4 2021/Q1 2022, where IoT services might be regulated separately.

The current implication of ePD on IoT services is that even when Traffic Data or Content Data is not Personal Data, it is still subject to specific confidentiality obligations and restrictions in terms of certain types of processing. But that is for Telia to comply with.