SHUber – Data Protection Considerations

Data Protection – Considerations Regarding Usage & Sharing of Data

Since SHUber deals with both locations and payment details, there is a lot of potential for dangerous mishap in the storage, processing and sharing of its users' data. Personal, sensitive, and other types of data and the regulations surrounding their storage and processing are outlined by GDPR, available to view in full at gdpr-info.eu (Intersoft Consulting, 2018).

While sensitive data must be treated with the utmost regard for privacy, there also must be a balance found between a complete lockdown of all data and an acceptable level of practicality in its use – if the data is too hard to access through the system then this may lead to other issues; if nothing else a lack of business due to a frustrating experience.

Sharing of user data should be tightly restricted, only granting access to certain parts of the data where necessary, for example sharing the pickup point with the driver based on the user's location – even then, the location might be generalised and not live (just a snippet of roughly where they were when they ordered the taxi).

SHUber ultimately handles a lot of 'personal data' (ICO, 2018) from each user, including up to:

- (Full) name
- Phone number
- Email address
- Home/work/other addresses
- Payment (card) details
- Drivers license & ID (for drivers)

As more and more apps include encryption algorithms and protocols in all data sent and received (Google, 2019), the SHUber app's traffic will be fully encrypted on both the customer's and driver's side of things, along with the central server(s).

That being said, the app & system still need to be carefully designed to protect sensitive data wherever it is being dealt with – from passing on a name from customer to driver, to issuing a bank transaction; all must occur in the most secure manner feasible.

To start with, the user's phone number and email address would not need to be accessed by any other user of the app – they would strictly be for control and management of their account – there should be no way to access this information through the app except if logged in as the user themselves through the account settings/info page.

Saved user addresses are obviously sensitive in that they most likely outline where the customer lives, works, has friends that live, etc… regardless they could definitely be traced back to the user and misused with malicious intent so the data is sensitive and must be protected. This presents a fairly obvious dilemma though, in the fact that the driver of a taxi has to know where to go – we must provide them with an address, but we protect the data by removing it from any context: all they know about the customer is their first name and somewhere they wanted to go on a certain occasion – this is the minimal risk we can achieve whilst still having a functional service.

Payment card details will be stored securely in the SHUber app, on the user's own device but still encrypted. We simply save them here so the user doesn't have to enter them manually every time. SHUber will employ a 3rd party to process the transaction so that matter is out of our hands, beyond choosing an appropriate company. However this company would need to conform to standards like the PCI DSS (IT Governance, 2019).

When a driver signs up to SHUber they must provide proof of eligibility to drive, and for legal reasons SHUber will keep a copy of these documents securely on its own servers. This data should never need to be accessed though except manually, and internally, when retrieving a driver's documents for some special reason.

Data Processing – What Happens Where?

When a SHUber customer requests a taxi, a snippet of their location is captured by the app on their phone and submitted to the SHUber server along with their ride request. This happens in a secure manner using modern encryption standards, as stated above in regard to encrypted app traffic.

The information created at this initial step is limited to a snippet of the customer's location and the address of where they want to go in the taxi.

The request is shown to all nearby drivers on their devices who can opt to accept or decline the trip; when one accepts it the offer will then disappear for the rest and they will be locked in as the driver for the trip. They are sent a pickup location and some limited information about the customer (name, also rating if they have one) to help ensure they pick up the right person.

Now that the customer is in the taxi and the driver knows where they want to go, the trip follows. The driver confirms the completion of the trip through their app upon arrival and the customer gets out at their destination.

Then, based on various factors such as demand and traffic severity, a fare multiplier is calculated by the driver's app (the driver themselves has no influence in this) and the customer's fare is calculated and charged to their specified payment details.

Remember that we complete the transaction using a 3rd party payment management company, we just securely send them the card details and transaction amount and they handle the rest.

Finally both the customer and driver get in-app prompts to rate their experience with the other on a 5-star scale. These results are uploaded to the SHUber server and update their user profiles.

References

Google. (2019, 12 3). *An Update on Android TLS Adoption*. Retrieved from Google Security Blog: https://security.googleblog.com/2019/12/an-update-on-android-tls-adoption.html

ICO. (2018). *Guide to the GDPR: What is personal data?* Retrieved from Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

Intersoft Consulting. (2018). *General Data Protection Regulation (GDPR)*. Retrieved from Intersoft Consulting: https://gdpr-info.eu/

IT Governance. (2019). *The PCI DSS (Payment Card Industry Data Security Standard)*. Retrieved from IT Governance: https://www.itgovernance.co.uk/pci_dss