Traka Products: General Data Protection Regulations (GDPR) FAQ

Date: 9 February 2018

Q. ***How is Traka preparing for the introduction of GDPR in May 2018?***

A. Traka, as part of ASSA ABLOY Ltd, has been actively working on the preparations for GDPR since May 2017 and this work is planned to achieve two primary objectives. Firstly, to ensure that Traka as a business will be fully compliant with GDPR when it is introduced. Secondly, to make sure that Traka systems enable our clients to store and process personal data in line with the requirements of GDPR.

Traka products covered by this document: All current products, ie: Traka 8/16-bit key cabinets and lockers; Traka "simple locker systems"; Traka Touch key cabinets and lockers; Traka immobiliser products; Traka 32 software; Traka Web software; Traka "Packaged Integrations" and "Integration Engine (v2)"; Traka 21 key cabinet; Traka Automotive (eTag) products; TACLS/RTUS; Traka 8/16-bit "pods" (used for access control).

The following product options are outside the scope of this document at the moment:

- Systems with "card readers" or other token-readers where the reader was supplied and fitted by anyone other than Traka, or where the reader was chosen by the client and supplied ("free issued") to Traka and fitted to the system at the client's request are excluded in respect of those readers because Traka was not responsible for that functionality (although from our general understanding, we have no specific concerns).
- Systems with "Alcolock" functionality are excluded because we are still investigating the GDPR implications of the data involved.
- Systems with Sagem, TSSi or any other make of "finger reader" supplied by Traka as part of a Traka system are excluded from this document for the time being, because we are still investigating whether the data item transmitted from these readers counts as a "Digital ID" (ie Personal Data) or as "biometric data" (ie Sensitive Personal Data).

Q. ***What do Traka products do?***

A. Traka supplies Key Cabinets and intelligent Locker systems. These products keep the keys/assets safe from unauthorised access, and allow authorised users to remove and return the keys and assets they are entitled to (which might change, minute by minute, for many reasons). Traka systems give full accountability of who has (or had) which keys at what time. This is usually managed by a Traka software product that runs on the client's computer network. To achieve all this, the Traka products hold information about the users and the keys/items – the user's names, ID card numbers, the keys and items they are entitled to, and so on.

Q. ***Do Traka systems store and process Personal Data?***

A. Yes, in almost all cases. The amount and type of personal data held within a Traka system is defined by the business or organisation that uses the system (the "Data Controller") and is not determined by Traka or the system itself. The Personal Data can be as simple as just the name & PIN or card number of individual users, or more detailed personal information can be held within the systems if the client requires it.

Q. ***Do Traka systems store and process Sensitive Personal Data?***

A. No, in most cases. The client is responsible for identifying whether any of the Personal Data it holds and processes in its Traka system is Sensitive Personal Data, and if so, the client must implement the higher levels of control and documentation required.

We are currently investigating the data associated with the Sagem and other "finger readers" so we can assist our clients in their deliberations about whether to treat this data as Personal Data or Sensitive Personal Data. Currently these product options are outside the scope of this document.

Q. ***Do Traka systems fulfil the data protection principles of GDPR?***

A. Article 5(2) of the GDPR requires that the Data Controller (in this case, Traka's client, the organisation using the Traka system) "shall be responsible for, and be able to demonstrate, compliance with the principles". In our opinion, the functionality of all Traka systems is entirely compatible with the GDPR data protection principles, however it is the client's responsibility to ensure that their usage of their Traka systems fulfils those principles, and that this can be demonstrated.

Q. **What is the "lawful basis for processing" personal data within a Traka system?**

A. It is the responsibility of the Data Controller (in this case, Traka's client) to determine which of the six available lawful bases for processing personal data applies to their situation. From what we know of our clients and the way those organisations use their Traka products, we anticipate that "Legitimate Interest" will be the most frequently used lawful basis for processing: the legitimate interest of an organisation to control access to its keys and assets, to be able to monitor who holds/held those items at any moment in time; the processing of a user's name and entitlements to achieve this, and the user's reasonable expectations that their name etc will be used for this purpose.

Q. ***How do Traka systems help achieve the "individual rights" under GDPR?***

A. The individual has a "**Right to be informed**" of how their personal data is being used within the Traka system. The client organisation will typically fulfil this responsibility through a privacy notice

The individual has a "**Right of access**", to their personal data being held in the system. Traka systems have facilities to show information to users on the screen or to print out information for an individual user

The individual has a "**Right of rectification**", if their personal data held within the Traka system is inaccurate or incomplete. Traka systems contain functionality to allow the organisation to make such changes to the data within the system and in most cases, it will be in the organisation's interest to correct any inaccuracies (an employee's name mis-spelt, an employee's entitlement to keys or other assets incorrectly recorded).

The individual has a "**Right to erasure**", also known as the "**right to be forgotten**". There are some circumstances where this right does not apply, and extra attention is required where the user is/was a child. Traka systems contain facilities to delete user's names and all other personal data. Traka systems also allow for a user's name to be pseudonymised, if the client organisation wishes to retain details of that user's activities (eg keys or assets being removed) but without retaining the user's actual name (eg, replace the name with "Former Employee number 917"). Client organisations will need to decide how an individual's "right to erasure" will be implemented in respect of its various data backups, including backups of data from its Traka systems. As with many other IT systems, most data deletion within Traka systems consists of flagging the relevant material as having a status of deleted, rather than physically erasing the information from the computer disk. We will be happy to provide further advice/consultancy on various possible methods of more physical data destruction.

The individual has a "**Right to restrict processing**" in some circumstances. Traka contains numerous facilities that can be used to achieve this, in various circumstances. In particular, setting a user as "inactive" may achieve exactly what is required in many situations.

The individual has a "**Right to data portability**" – to get a "copy" of their personal data being held within the Traka system to use on some different computer system. Traka has various facilities to "output" a copy of a user's personal data which we believe collectively will enable our clients to fulfil this obligation. In many cases, the only personal data held in the system will be the user's name and perhaps a PIN number of staff card number. We therefore anticipate that individual users of Traka systems within their workplace or educational establishment will not often want to utilise this right to get a copy of their data from the system.

The individual has a "**Right to object**" (to their personal data being processed) in various circumstances, and in some cases, use of the data must cease immediately, while the objection is being investigated. Traka systems contain various facilities to enable the client to do this.

The individual has "**Rights related to automated decision-making**". We believe that the functionality of Traka systems, controlling the issuing and return of keys and assets to authorised users, does not normally comprise automated decision-making within the meaning of Article 22. An individual's entitlement to keys or assets is set manually, by an administrator. The only thing that happens automatically is the system identifying the user (from their PIN, staff card or similar), and a key or item being released (or returned). However if one of our client organisation concludes that its use of its Traka products falls within Article 22, that organisation will have to implement the required additional processes and documentation.

Q. ***How do Traka systems apply the "security" principles of GDPR?***

A. Detailed guidance on this topic within the context of GRPD has not yet been issued by the ICO, and their website redirects visitors to their earlier guidance notes for the Data Protection Act, and specifically Principle 7. The organisation should put in place security measures that seek to ensure

- only authorised people can access, alter, disclose or destroy personal data;
- those people only act within the scope of their authority; and
- if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned

The Act says you should have security that is appropriate to:

- the nature of the information in question; and
- the harm that might result from its improper use, or from its accidental loss or destruction.

We believe that the only Personal Data that most of our clients will process in their Traka Systems will be user's names and ID card numbers. Some clients will store other types of Personal Data. In general, this data will normally be at the least sensitive and least harmful end of the spectrum, compared to other types of Personal Data in other systems.

We believe that the facilities within Traka systems enable our clients to fulfil these obligations, when considered in the context of physical access control to the business premises containing the Traka systems, and typical IT network security arrangements (passports, screen savers, confidential waste disposal including shredding) and back-up arrangements. However it remains the client's responsibility to ensure that its arrangements and procedures are fit for this purpose.

Q. How do Traka systems apply the "data protection by design & default" principles of GDPR?

A. As of January 2018, the UK ICO's website refers readers to a 2013 "Privacy by Design" paper from the Information & Privacy Commissioner of Ontario, Canada, available at the following link:

https://www.ipc.on.ca/resource/privacy-by-design/

This paper sets out the following seven "foundation principles":

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the default setting
3. Privacy embedded into Design
4. Full functionality – positive-sum not zero-sum
5. End-to-End Security – Full lifecycle protection
6. Visibility and Transparency – Keep it Open
7. Respect for User Privacy – Keep it User-Centric

We believe that the facilities within Traka systems enable our clients to fully implement these "privacy by design & default" principles.

Q. How are Personal Data Breaches handled in connection with Traka systems?

A. An organisation using Personal Data for any purpose must have written procedures for handling any form of Personal Data Breach, and these procedures should include possible data breaches from its Traka systems. We believe the functionality of Traka products and the types of Personal Data that they use will mean that the Traka systems are a relatively low risk, in terms of possible data breaches, compared with many other systems in use in most organisations.

The Traka systems in use within an organisation may help reduce and/or detect data breaches. A Traka key cabinet will enable the organisation to know who took the key to the server room, and will prevent unauthorised employees using that key. A Traka intelligent laptop locker will record who used a pooled laptop, in a corporate hot-desk environment.

Q. How is "Personal Data at rest" protected within Traka systems?

A. Traka solutions are made up of several components including software, hardware and databases. The information below outlines the physical and virtual aspects of the product in relation to data at rest.

- Physical Security:
  - Traka Web / Traka32 / eTag
    - The central database containing personal data (such as Forename, Surname, 10 x User definable field that could be used to store personal data, Card ID, Keypad ID and/or PIN) typically resides on a PC or Server installed with Microsoft SQL Server.

        - Physical access to the server is controlled by the client, for example by storing the Server in an access controlled server room.
        - Virtual access to the server and database contained within is controlled by user account credentials granting or denying access to the operating system and/or SQL server.
    - Traka Touch
        - The local database containing a subset of personal data (such as Forename, Surname, Card ID, Keypad ID and/or PIN) resides in Flash Memory which is integral to the Motherboard and cannot be removed.
        - Rolling database backups optionally reside on a removable SD card however the SD card is only accessible by opening the Pod using an override key.
        - Some Traka Touch systems are fitted with USB Sockets to order to extract database backups and export user information in the form of a Microsoft Excel spread sheet. Data can only be extracted with the relevant Administrative privileges.
    - All other hardware products
        - The local database containing a subset of personal data (such as Forename, Surname, Card ID, Keypad ID and/or PIN) resides in Battery backed RAM or Flash Memory which is integral to the Motherboard and cannot be removed.
        - There is no way to extract data from the Battery backed RAM or Flash Memory.

- Virtual Security:
    - Traka Web / Traka32 / eTag
        - All data accessible through Traka Web and Traka32 is restricted behind logins to the software and in turn the login is associated with a set of permissions at to what the login can or cannot see.
    - Central Databases
        - Traka Web encrypts Card ID's, PIN's and Passwords within its central SQL database.
        - Traka32 has the optional ability to encrypt the entire database when used with SQL Server.
        - eTAG software does not encrypt any data stored within the database.
    - Local database (within the Traka key cabinet or locker)
        - Traka Touch encrypts Card ID's, PIN's and Passwords within its local database.
        - 8/16bit systems do not encrypt any data stored within the database.

Q. ***How is "Personal Data in transit" protected within Traka systems?***

A. When data is transmitted between Traka components, certain levels of data protection in the form of encryption have been applied. The information below outlines the levels of encryption in relation to data in transit.

- Traka Web Client to Traka Web Business Engine
    - Data can be encrypted with certificates to HTTPS

- Traka Web Business Engine to Traka Web Database
  - The level of encryption depends on the SQL configuration.
  - Data such as Card ID, Keypad ID, PINs and Passwords are encrypted at rest in the database and as such remain in their encrypted states when transmitted between the BE and the database.
- Traka Web Business Engine to Traka Web Comms Engine
  - All data transmitted between the BE and the CE is encrypted using Message Security to AES256.
- Traka Web Comms Engine to Traka Touch
  - All data transmitted between the CE and the TT is encrypted using Transport Layer Security 1.0.
- Traka32 Client to Traka32 Database
  - The level of encryption depends on the SQL configuration.
- Traka32 Client to 8/16bit System
  - Data can be encrypted to AES256 dependant on the network adaptor fitted to the unit.
- eTag Client to eTag Database
  - The level of encryption depends on the SQL configuration.
- eTag Client to 8/16bit System
  - There is no encryption available on this system. Data such as Forename, Surname, Card ID, Keypad ID and PINs are sent in clear text.

Q. Is Traka intending to make any changes to its products to assist clients fulfil their GDPR obligations?

A. Yes. Although we are confident that our clients can already fulfil all their GDPR obligations in connection with their Traka products, we are looking at product enhancements that will simplify some of the administrative processes and further strengthen some aspects of data security. Possibilities we are currently considering include:

1. Enhanced functionality for a "hard delete" of data (including user details, ie personal data) from Traka products;
2. Further enhancements and/or suggested procedures for deleting or anonymising user details while retaining utilisation data for the keys or assets within the Traka systems that those deleted users had accessed.
3. New functionality to invite a user to give consent prior to enrolling the user's finger, in those Traka Touch/Web systems that include a finger reader as a method of user authentication. The consent will be stored and will be available for future auditing/reporting
4. Higher levels of encryption to be made available for some types of data
5. Minimum password lengths, specified password complexity, and regular password change regimes, for access to Traka Web software

We would welcome views from our clients on the relative importance of the above possible new functionality, or on anything else that we should consider. We envisage including some of the above features into our development roadmap from late 2018 onward. We would reiterate, we are confident that the existing functionality of our products fully enables all our clients to meet their obligations as Data Controllers under GDPR.