Annex 2 - Technical and organisational measures

Processor has taken the following organisational measures:

- All processor employees have signed a confidentiality agreement.
- Employees are made aware of the rules around data breaches and security. This is part of the onboarding process.
- All processor employees are aware of the importance of protecting of personal data. Every week during the work meeting there is an opportunity to ask questions or make comments about this.
- A strict password policy is in place and a password manager in which all passwords are stored. Complex passwords are chosen and these are stored encrypted.
- When employees leave employment, important passwords are changed immediately and access to the password manager is blocked.
- Once processors terminate their relationship with processors, processors will transfer the controller's personal data. As soon as the data have been transferred, processor shall within 30 working days transfer all personal data of the controller's relations from its systems.
- The personal data of the processing controller and the contacts of controller will be retained in processor's systems for 7 years due to legal obligations.
- Processor works with sub-processors. Processor has, where possible, concluded processing agreements with these sub-processors.
- Where possible, Processor works with 2FA (two factor authentication).

RouteLogic advises Processor to:

- Always perform mandatory (software) updates and use the latest software version use.
- Activate 2fa for account login on app.routelogic.io.
- Set hard-to-guess passwords for RouteLogic access.
- Use a password manager to choose different and difficult passwords
- The default retention time of personal data in RouteLogic is 30 days. If possible, we recommend setting the retention time as short as possible.