# Data Processing Agreement (version 1.3)

Between

The CUSTOMER (The data controller)

and

**"Tjekvik"**

**Autoinnovation ApS**
Kronprinsessegade 6
1306 Copenhagen K
Denmark
VAT: DK37211192
(+45) 3070 6970
admin@tjekvik.com

(the data processor)

each a "party"; together "the parties"

HAVE AGREED on the following Contractual Clauses (the Clauses) to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

## 1. PREAMBLE

1.1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

1.2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

1.3. In the context of the provision of "Tjekvik, digital service reception" the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

1.4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

1.5. Three appendices are attached to the Clauses and form an integral part of the Clauses.

1.6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

1.7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorized by the data controller.

1.8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum-security measures to be implemented by the data processor and how audits of the data processor and any sub- processors are to be performed.

1.9. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

1.10. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

## 2. THE RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

2.1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 in the GDPR), the applicable EU or Member State data protection provisions and the Clauses.

2.2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

2.3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

## 3. THE DATA PROCESSOR ACTS ACCORDING TO INSTRUCTIONS

3.1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also
be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

3.2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

## 4. CONFIDENTIALITY

4.1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to per- sons under the data processor's authority who have commit- ted themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis. The list of persons to whom access has been granted shall be kept under periodic review. Based on this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

4.2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality

## 5. SECURITY OF PROCESSING

5.1. Article 32 in the GDPR stipulates that, considering the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

a. Pseudonymisation and encryption of personal data;

b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5.2. According to Article 32 in the GDPR, the data processor shall also
– independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

5.3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 in the GDPR, by inter alia providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 in the GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 in the GDPR.

If subsequently – in the assessment of the data controller
– mitigation of the identified risks requires further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 in the GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

## 6. USE OF SUB-PROCESSORS

6.1. The data processor shall meet the requirements specified in Article 28(2) and (4) in the GDPR to engage another processor (a sub-processor).

6.2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

6.3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replace- ment of sub-processors at least 6 weeks in advance in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

6.4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

6.5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6.6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e. g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

6.7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – those foreseen in Articles 79 and 82 in the GDPR – against the data controller and the data processor, including the sub-processor.

## 7. TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

7.1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur based on documented instructions from the data controller and shall always take place in compliance with Chapter V in the GDPR.

7.2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, are required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

a. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

b. transfer personal data to a data controller or a data processor in a third country or in an international organ- ization
c. transfer the processing of personal data to a sub-processor in a third country
d. have the personal data processed by the data processor in a third country

7.3. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V in the GDPR on which they are based, shall be set out in Appendix C.6.

7.4. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V in the GDPR.

## 8. ASSISTANCE TO THE DATA CONTROLLER

8.1. Considering the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III in the GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

a. the right to be informed when collecting personal data from the data subject

b. the right to be informed when personal data have not been obtained from the data subject

c. the right of access by the data subject

d. the right to rectification

e. the right to erasure ('the right to be forgotten')

f. the right to restriction of processing

g. notification obligation regarding rectification or erasure of personal data or restriction of processing

h. the right to data portability

i. the right to object

j. the right not to be subject to a decision based solely on automated processing, including profiling

8.2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, considering the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority relevant to the data controller, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons; the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

b. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

c. the data controller's obligation to consult the competent supervisory authority, relevant to the data controller prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

8.3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

## 9. NOTIFICATION OF PERSONAL DATA BREACH

9.1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

9.2. The data processor's notification to the data controller shall, if possible, take place within 24 HOURS after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 in the GDPR.

9.3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) in the GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

a. The nature of the personal data including where possible, the categories and approximate number of data

subjects concerned and the categories and approximate number of personal data records concerned;

b. the likely consequences of the personal data breach;

c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

9.4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

## 10. ERASURE AND RETURN OF DATA

10.1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data**.**
The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

## 11. AUDIT AND INSPECTION

11.1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

11.2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7.

11.3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

## 12. THE PARTIES' AGREEMENT ON OTHER TERMS

12.1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e. g. liability, if they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

## 13. COMMENCEMENT AND TERMINATION

13.1. The Clauses shall become effective on the date of both parties' signature.

13.2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

13.3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

13.4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

## 14. CONTACT POINT FOR THE DATA PROTECTION RESPONSIBLE

14.1. The controller may at any time contact the Data Protection Responsible at Tjekvik regarding the processing of personal data carried out by the processor. The Data Protection Officer can be reached by email: legal@tjekvik.com.

## 15. SIGNATURE

On behalf of the data controller the Data Protection Agreement is applied according to the specifiers in terms and conditions.

On behalf of the data processor

Name Christian Mark
Position CEO

Signature

# APPENDIX A

## INFORMATION
about the processing

The processing of personal data by Tjekvik, the data processor, for the Controller, limits itself to art. 6 data.

Personal data, regarding the costumers of the data controller, is deleted within 15 days.

Personal data, in regard to the employees of the Controller (names, email addresses and user roles), is processed by Tjekvik to ensure that the individual user has the correct access to the Tjekvik backend. The users and their data can be maintained directly by the account administrator (centrally across several workshops) or shop managers (local workshop manager). The data is stored, for as long as the data controller needs the data.

### A.1.
### THE PURPOSE OF THE DATA PROCESSOR'S PROCESSING OF PERSONAL DATA ON BEHALF OF THE DATA CONTROLLER IS:

The product is an intuitive self-service technology for the automotive industry, that lets the customers check-in and out how, when and where they want – at home, in the dealership by the indoor kiosk or securely outdoor by the outdoor kiosk.
The customer checks in and out with phone number or license plate.

The data is processed in order to:

- Allow the customer to begin check-in before the scheduled appointment starts
- Allow the customer to use self-service during check-in
- Allow the customer to use self-service during check-out

### A.2.
### THE DATA PROCESSOR'S PROCESSING OF PERSONAL DATA ON BEHALF OF THE DATA CONTROLLER SHALL MAINLY PERTAIN TO (THE NATURE OF THE PROCESSING):

- Collection,
- recording,
- organization,
- structuring,
- storage,
- retrieval,
- use,
- alignment or combination,
- restriction,
- erasure or destruction.

### A.3.
### THE PROCESSING INCLUDES THE FOLLOWING TYPES OF PERSONAL DATA ABOUT DATA SUBJECTS:

- Name,
- address,
- e-mail,
- telephone number,
- registration number
- VIN number
- details about the specific vehicle, i. e. brand, model
- Order details, i. e. content of the planned work and in some cases price

## A.4.
## PROCESSING INCLUDES THE FOLLOWING CATEGORIES OF DATA SUBJECT:

- Current workshop customers of the data controller.
- Employees of the data controller.

## A.5.
## THE DATA PROCESSOR'S PROCESSING OF PERSONAL DATA ON BEHALF OF THE DATA CONTROLLER MAY BE PERFORMED WHEN THE CLAUSES COMMENCE. PROCESSING HAS THE FOLLOWING DURATION:

The duration of each processing for the data subject is generally 9 days, from when the processor import the data from a API. After 9 days, the system erases the personal data.

In certain instances, we process the data for a maximum of 15 days. This occurs when the processor import the data from a CSV system, and not an API solution.

# APPENDIX B

## AUTHORISED
sub-processors

### B.1.
### APPROVED SUB-PROCESSORS
On commencement of the Clauses, the data controller authorizes the engagement of the following sub-processors:

| NAME | CVR | ADDRESS | DESCRIPTION OF PROCESSING | LEGAL GROUND |
|---|---|---|---|---|
| **HEROKU** | **US TAX number:**<br>26-1088476<br>**Company number:**<br>C3096268 | Heroku is a part of Salesforce, and the HQ is located here:<br>415 Mission Street Suite 300 San Francisco, CA 94105 | Cloud hosting of the Tjekvik application (on AWS servers)<br>AWS DUB2 is located at 4033 Citywest Avenue, Cooldown Commons, County Dublin, Ireland and the Amazon AWS Amazon AWS FRA54 redundancy center is located at Eschborner Landstraße 100, 60489 Frankfurt am Main, Germany.<br>Personal data of your customers does not leave the EU. | Salesforce, including Heroku, that is a US-based sub-processor has certified to the US Department of Commerce that it complies with the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) regarding the processing of personal data received from the European Union and the United Kingdom in trust of the EU-U.S. |
| **AMAZON** | **Company number:**<br>C3568304 | HQ:<br>410 Terry Avenue North, Seattle, WA 98109-5210 | Cloud hosting of the SFTP server used for appointment imports via CSV files<br>The European region is located within Amazon Web Services' major Euro data center hub in Ireland.<br>4033 Citywest Avenue, Cooldown Commons, County Dublin, Ireland and the Amazon AWS Amazon AWS FRA54 redundancy center is located at Eschborner Landstraße 100, 60489 Frankfurt am Main, Germany.<br>Personal data of your customers does not leave the EU. | Amazon has certified to the US Department of Commerce that it complies with the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) regarding the processing of personal data received from the European Union and the United Kingdom in trust of the EU-U.S. |
| **TWILIO** | **Company number:**<br>10994798-0143 | HQ:<br>375 Beale Street Suite 300 San Francisco, CA<br>94105 USA | SMS operations<br>The server is located in the United States.<br>Twilio's default Region is in the eastern United States (US), US1 region. | Twilio has certified to the US Department of Commerce that it complies with the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) regarding the processing of personal data received from the European Union and the United Kingdom in trust |

of the EU-U.S.

| | | | | |
|---|---|---|---|---|
| **Or (you as a customer choose provider)** | | | | |
| **SINCH SWEDEN AB** | 556747-5495 | Lindhagensgatan 74<br>112 18 Stockholm<br>Sweden | The server is located within the EU/EEA in Dublin, Ireland and Frankfurt, Germany. | |
| **Mailgun** | **Company number:**<br><br>0802653513 | 112 E Pecan St.<br>#1135 San Antonio,<br>TX 78205, USA | E-mail operations<br><br>Datacenter and server is located in Germany.<br><br>Personal data of your customers does not leave the EU. | . |

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party.

In the absence of a decision pursuant to Article 45 (3), a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available, cf. Article 46 (1) of the Regulation. Appropriate safeguards have been implemented with the above-mentioned sub-processors, to ensure the rights of the data subject.

Tjekvik's US-based sub-processors have certified to the US Department of Commerce that they adhere to the EU-U.S. Data Privacy Framework Principles (EU-U.S., regarding the processing of personal data received from the EU and the UK in trust for the EU-U.S.

Other legal basis for transfer is based the European Commission's Standard Contractual Clauses (also known as EU model clauses), which provide specific guarantees regarding transfers of personal data for services within their scope. The EU model clauses are used in agreements between service providers (such as Mailgun) and their customers (the data processor) to ensure that all personal data leaving the EU is transferred in accordance with the GDPR.

Since the EU Commission's Standard Contractual Provisions require the data controller to be a direct party to the Standard Contractual Provisions, Tjekvik is authorized to enter into this on behalf of the data controller. As Mailgun is located in a third country, the EU Commission's Standard Contract Provisions are used as a valid legal basis for transfer.

On 4 June 2021, the Commission issued modernized Standard Contractual Clauses (SCC) under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR). See COMMISSION IMPLEMENTING DECISION (EU) 2021/914.

All personal data processed on behalf of the controller is processed within the territory of the EU/EEA.

## B.2.
## PRIOR NOTICE FOR THE AUTHORISATION OF SUB-PROCESSORS

If Tjekvik adds a sub processor to perform tasks where Tjekvik is the data processor on behalf of the data controller specified in this contract, prior notification will be given to the data controller no later than 6 weeks before the change of the sub-data processor takes place.

If the data controller has objections to the change, the objection should be made as soon as possible and no later than 21 days after the data controller has received the notification.

Any change in relation to the current approved data sub-processors is made by drawing up an allonge, which is signed by both parties and subsequent added as an appendix to this Data Processor Agreement.

# APPENDIX C

## INSTRUCTION PERTAINING
to the use of personal data

### C.1.
### THE SUBJECT OF/INSTRUCTION FOR THE PROCESSING
The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

The data processor processes the personal in order to provide "Tjekvik, digital service reception" to the data controller in accordance with the Terms of Service.

The data Tjekvik collects is derived from the Controllers DMS system or API. In rare instances data is collected from the data subject – which ensures right to rectification and that the data processed is correct.

The personal data will be subject to several processing activities, including but not limited to:

### C.2.
### SECURITY OF PROCESSING
The level of security shall take into account:

That the processing involves a significant amount of personal data, which are subject to Article 6 under the Regulation. No Article 9 or 10 data is processed. There is a low risk of the rights and freedoms of the data subject to be infringed, which considered the level of security reflects this.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

C.2.1. The data protection is handled by the CTO and the Head of Legal as stated in this document.

Tjekvik educates employees in the protection of personal data within the organization.

C.2.2. Requirements for encryption of personal data:

By default, Tjekvik uses HTTPS between an API and for user accounts. User passwords are also encrypted in the database.

Content transmitted over the network is always transmitted over HTTPS, using a 2048-bit public key certificate. SSLv3 and below, as well as TLS 1.0, is disabled considering the published vulnerabilities in these versions and the security implications thereof**.**

When data is transferred between systems, they are encrypted in transit (SFTP/HTTPS), there is an option for dealers to buy further encryption (encrypted data at rest inside the database).

C.2.3. Requirements for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services:

- Collection,
- recording,
- organization,
- structuring,
- storage,
- retrieval,
- use,
- alignment or combination,
- restriction,

- erasure or destruction.

Tjekvik has made it possible for data subjects to rectify information, such as contact information.

Tjekvik has made it possible for shop- and account administrators to add, rectify or delete information.

Full back-up of data is performed every 6 hours, delta backup in between.

C.2.4. Requirements for the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident:

Tjekvik only stores a very limited amount of data for a very limited period. If required, due to a physical or technical event, lost data can be re-imported and made available again.

C.2.5. Requirements for processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing:

A penetration test is performed on a recurrent basic, to ensure, that all personal data is stored safe within the system.

All employees are instructed in the guidelines regarding processing of personal data.

C.2.6.

**The Access Management**

**Physical Access Control**
Tjekvik is a full remote company. No infrastructure is hosted at an office or a facility.
Tjekvik platform is cloud based and all PAC policies are handled by Heroku and AWS and treated according to the official standards.

**System Access Control**
Access to digital resources is limited to the people needing it: 1st level and 2nd level support mainly, and DevOps team.
Security is ensured by use of SSH keys and user login with strong password policy and/or MFA.

**Data Access Control**
Access to data resources is limited to the people needing it: 2nd level support in read-mode only in production.
Security is ensured by use of SSH keys and user login with strong password policy and/or MFA.

**Data Transmission Control**
Content transmitted over the network is always transmitted over HTTPS, using a 2048-bit public key certificate. SSLv3 and below, as well as TLS 1.0, is disabled in light of the published vulnerabilities in these versions and the security implications thereof.

**Input Control**
- Data imported (for appointments) from External systems are checked for consistency and SQL injection attacks
- Input Control are secured by the use of specific recognized libraries which are used at every build of the platform before deployment to test and detect input control vulnerabilities.
- A penetration testing (operated by Sapphire company) was performed in 05/2022. No CRITICAL issue was detected, all HIGH detected issues have been solved in Q3/2022 and launched in production. Penetration tests will be organised every 2 years.

**Availability Control**
An alert system is in place if the platform would go down (all components are monitored and alerting separately)
Failover and Redundancies will be implemented in 2024 after Infrastructure is fully moved to AWS (today, part in Heroku and part in AWS).

## C.3.
## ASSISTANCE TO THE DATA CONTROLLER

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

Tjekvik will notify the data controller, if possible, within 24 HOURS after Tjekvik has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

## C.4.
## STORAGE PERIOD/ERASURE PROCEDURES

The general storage period is 14 days. If a data subject has not picked up their vehicle key, their data is not deleted before, their key has been picked up.

The period can be extended if the appointment import source is from a CSV file, since we then keep the appointments used for check-in for 25 days, to secure availability for checkout.

## C.5.
## PROCESSING LOCATION

Processing of the personal data under the Clauses will be performed at the locations stated in B.1, and at the office of Tjekvik.

## C.6.
## INSTRUCTION ON THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Upon transferring data to a third country, which either has an adequate level of protection (a safe third country) or to a third country without a level of security in accordance with the General Data Protection Regulation, all transfers have a legal basis of transferring.

In regards to transfers of personal data to third countries that are not on the list of safe third countries, Tjekvik will continuously and atleast annually, follow up on whether the data processor still meets the security requirements in regards to the transferring of personal data to third countries, set forth in the General Data Protection Regulation. Should it be the case that the requirements of the regulation are not complied with, Tjekvik will immediately terminate the cooperation with the sub processor and inform the Controller of the decision to terminate the cooperation. When changing a sub processor, Tjekvik will use the agreed procedure set forth in B.2

## C.7.
## PROCEDURES FOR THE DATA CONTROLLER'S AUDITS, INCLUDING INSPECTIONS, OF THE PROCESSING OF PERSONAL DATA BEING PERFORMED BY THE DATA PROCESSOR

The data controller or the data controller's representative shall be entitled to perform a annual physical inspection of the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing to ascertain the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

In addition to the planned inspection, the data controller may perform an inspection of the data processor when the data controller deems it required.