

Acordo de Processamento de Dados (versão 1.3)

NOTA SOBRE O IDIOMA: Este documento é uma tradução do original em inglês fornecida para conveniência. Em caso de conflito ou divergência entre a versão portuguesa e a versão inglesa, a **versão em inglês prevalece**.

Entre

O CLIENTE (O responsável pelo tratamento de dados)

e

"Tjekvik"

Autoinnovation ApS, Tjekvik
Kronprinsessegade 36, 1.
1306 Copenhagen K
Dinamarca
NIF: DK37211192
(+45) 3070 6970
legal@tjekvik.com

(o subcontratante)

cada um "parte"; em conjunto "as partes"

ACORDARAM as seguintes Cláusulas Contratuais (as Cláusulas) para cumprir os requisitos do RGPD e para assegurar a proteção dos direitos do titular dos dados.

1. PREÂMBULO

1.1. Estas Cláusulas Contratuais (as Cláusulas) estabelecem os direitos e obrigações do responsável pelo tratamento de dados e do subcontratante, quando este processa dados pessoais em nome do responsável pelo tratamento de dados.

1.2. As Cláusulas foram elaboradas para assegurar a conformidade das partes com o Artigo 28(3) do Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

1.3. No contexto da prestação do serviço "Tjekvik, receção digital de serviços", o subcontratante irá processar dados pessoais em nome do responsável pelo tratamento de dados, em conformidade com as Cláusulas.

1.4. As Cláusulas prevalecerão sobre quaisquer disposições semelhantes contidas noutros acordos entre as partes.

1.5. Três apêndices estão anexados às Cláusulas e fazem parte integrante das mesmas.

1.6. O Apêndice A contém detalhes sobre o processamento de dados pessoais, incluindo o propósito e a natureza do processamento, o tipo de dados pessoais, as categorias de titular dos dados e a duração do processamento.

1.7. O Apêndice B contém as condições do responsável pelo tratamento de dados para o uso de subcontratantes pelo subcontratante e uma lista de subcontratantes autorizados pelo responsável pelo tratamento de dados.

1.8. O Apêndice C contém as instruções do responsável pelo tratamento de dados relativamente ao processamento de dados pessoais, as medidas mínimas de segurança a implementar pelo subcontratante e a forma como as auditorias ao subcontratante e a quaisquer subcontratantes devem ser realizadas.

1.9. As Cláusulas, juntamente com os apêndices, devem ser conservadas por escrito, incluindo eletronicamente, por ambas as partes.

1.10. As Cláusulas não isentam o subcontratante das obrigações a que está sujeito ao abrigo do Regulamento Geral sobre a Proteção de Dados (RGPD) ou de outra legislação aplicável.

2. OS DIREITOS E OBRIGAÇÕES DO RESPONSÁVEL PELO TRATAMENTO DE DADOS

2.1. O responsável pelo tratamento de dados é responsável por garantir que o processamento de dados pessoais ocorra em conformidade com o RGPD (ver Artigo 24 do RGPD), as disposições aplicáveis de proteção de dados da UE ou do Estado-Membro, e as Cláusulas.

2.2. O responsável pelo tratamento de dados tem o direito e a obrigação de tomar decisões sobre as finalidades e os meios de processamento dos dados pessoais.

2.3. O responsável pelo tratamento de dados é responsável, entre outros aspetos, por garantir que o processamento de dados pessoais que o subcontratante é instruído a realizar tem base jurídica.

3. O SUBCONTRATANTE AGE DE ACORDO COM INSTRUÇÕES

3.1. O subcontratante deve processar os dados pessoais apenas com base em instruções documentadas do responsável pelo tratamento de dados, salvo se for obrigado a fazê-lo por legislação da União ou do Estado-Membro a que o subcontratante está sujeito. Tais instruções devem ser especificadas nos Apêndices A e C. Instruções subsequentes também podem ser dadas pelo responsável pelo tratamento de dados durante a duração do processamento dos dados pessoais, mas essas instruções devem ser sempre documentadas e mantidas por escrito, incluindo eletronicamente, em conexão com as Cláusulas.

3.2. O subcontratante deve informar imediatamente o responsável pelo tratamento de dados se, no entender do subcontratante, as instruções dadas pelo responsável pelo tratamento de dados violarem o RGPD ou as disposições aplicáveis de proteção de dados da UE ou do Estado-Membro.

4. CONFIDENCIALIDADE

4.1. O subcontratante deve conceder acesso aos dados pessoais processados em nome do responsável pelo tratamento de dados apenas às pessoas sob a autoridade do subcontratante que se comprometeram a respeitar a confidencialidade ou estão sujeitas a uma obrigação legal adequada de confidencialidade, e apenas numa base de necessidade de conhecimento. A lista de pessoas a quem foi concedido acesso deve ser sujeita a revisão periódica. Com base nesta revisão, tal acesso a dados pessoais pode ser retirado, se o acesso deixar de ser necessário, e os dados pessoais conseqüentemente não serão mais acessíveis a essas pessoas.

4.2. O subcontratante, a pedido do responsável pelo tratamento de dados, deve demonstrar que as pessoas relevantes sob a autoridade do subcontratante estão sujeitas à obrigação de confidencialidade acima mencionada.

5. SEGURANÇA DO PROCESSAMENTO

5.1. O Artigo 32 do RGPD estipula que, tendo em conta o estado da arte, os custos de implementação e a natureza, âmbito, contexto e finalidades do processamento, bem como o risco de probabilidade e gravidade variável para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento de dados e o subcontratante devem implementar medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco.

O responsável pelo tratamento de dados deve avaliar os riscos para os direitos e liberdades das pessoas singulares inerentes ao processamento e implementar medidas para mitigar esses riscos. Dependendo da sua relevância, as medidas podem incluir:

- a. Pseudonimização e encriptação de dados pessoais;
- b. a capacidade de garantir a contínua confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços de processamento;
- c. a capacidade de restaurar a disponibilidade e o acesso aos dados pessoais em tempo útil em caso de incidente físico ou técnico;
- d. um processo de teste, avaliação e verificação regulares da eficácia das medidas técnicas e organizativas para garantir a segurança do processamento.

5.2. Nos termos do Artigo 32 do RGPD, o subcontratante deve também — independentemente do responsável pelo tratamento de dados — avaliar os riscos para os direitos e liberdades das pessoas singulares inerentes ao processamento e implementar medidas para mitigar esses riscos. Para este efeito, o responsável pelo tratamento de

dados deve fornecer ao subcontratante todas as informações necessárias para identificar e avaliar tais riscos.

5.3. Além disso, o subcontratante deve assistir o responsável pelo tratamento de dados no cumprimento das suas obrigações ao abrigo do Artigo 32 do RGPD, fornecendo ao responsável pelo tratamento de dados informações sobre as medidas técnicas e organizativas já implementadas pelo subcontratante ao abrigo do Artigo 32 do RGPD, bem como todas as outras informações necessárias para que o responsável pelo tratamento de dados cumpra a sua obrigação ao abrigo do Artigo 32 do RGPD.

Se, na avaliação do responsável pelo tratamento de dados, a mitigação dos riscos identificados exigir medidas adicionais para além das já implementadas pelo subcontratante ao abrigo do Artigo 32 do RGPD, o responsável pelo tratamento de dados deve especificar essas medidas adicionais no Apêndice C.

6. UTILIZAÇÃO DE SUBCONTRATANTES

6.1. O subcontratante deve cumprir os requisitos especificados no Artigo 28(2) e (4) do RGPD para contratar outro subcontratante.

6.2. O subcontratante não deve, portanto, contratar outro subcontratante para o cumprimento das Cláusulas sem a autorização prévia e geral por escrito do responsável pelo tratamento de dados.

6.3. O subcontratante tem a autorização geral do responsável pelo tratamento de dados para a contratação de subcontratantes. O subcontratante deve informar por escrito o responsável pelo tratamento de dados de quaisquer alterações pretendidas relativas à adição ou substituição de subcontratantes com pelo menos 6 semanas de antecedência, dando assim ao responsável pelo tratamento de dados a oportunidade de se opor a tais alterações antes da contratação do(s) subcontratante(s) em causa. Prazos de aviso prévio mais longos para serviços de subcontratação específicos podem ser previstos no Apêndice B. A lista de subcontratantes já autorizados pelo responsável pelo tratamento de dados encontra-se no Apêndice B.

6.4. Quando o subcontratante contratar um subcontratante para realizar atividades de processamento específicas em nome do responsável pelo tratamento de dados, as mesmas obrigações de proteção de dados estabelecidas nas Cláusulas devem ser impostas a esse subcontratante mediante contrato ou outro ato jurídico ao abrigo do direito da União ou do Estado-Membro, fornecendo em especial garantias suficientes para implementar medidas técnicas e organizativas adequadas de forma que o processamento cumpra os requisitos das Cláusulas e do RGPD.

O subcontratante é, portanto, responsável por exigir que o subcontratante cumpra, pelo menos, as obrigações a que o subcontratante está sujeito ao abrigo das Cláusulas e do RGPD.

6.5. Uma cópia do acordo com o subcontratante e alterações subsequentes deve — a pedido do responsável pelo tratamento de dados — ser apresentada ao responsável pelo tratamento de dados, dando assim ao responsável pelo tratamento de dados a oportunidade de garantir que as mesmas obrigações de proteção de dados estabelecidas nas Cláusulas são impostas ao subcontratante. As cláusulas sobre questões comerciais que não afetem o conteúdo legal de proteção de dados do acordo com o subcontratante não requerem apresentação ao responsável pelo tratamento de dados.

6.6. O subcontratante deve acordar uma cláusula de terceiro beneficiário com o subcontratante onde — em caso de falência do subcontratante — o responsável pelo tratamento de dados seja um terceiro beneficiário do acordo com o subcontratante e tenha o direito de fazer cumprir o acordo contra o subcontratante contratado pelo subcontratante, por exemplo, permitindo ao responsável pelo tratamento de dados instruir o subcontratante a eliminar ou devolver os dados pessoais.

6.7. Se o subcontratante não cumprir as suas obrigações de proteção de dados, o subcontratante permanece totalmente responsável perante o responsável pelo tratamento de dados pelo cumprimento das obrigações do subcontratante. Tal não afeta os direitos dos titulares dos dados ao abrigo do RGPD — os previstos nos Artigos 79 e 82 do RGPD — contra o responsável pelo tratamento de dados e o subcontratante, incluindo o subcontratante.

7. TRANSFERÊNCIA DE DADOS PARA PAÍSES TERCEIROS OU ORGANIZAÇÕES INTERNACIONAIS

7.1. Qualquer transferência de dados pessoais para países terceiros ou organizações internacionais pelo subcontratante só pode ocorrer com base em instruções documentadas do responsável pelo tratamento de dados e deve sempre ocorrer em conformidade com o Capítulo V do RGPD.

7.2. Caso as transferências para países terceiros ou organizações internacionais, que o subcontratante não foi instruído a realizar pelo responsável pelo tratamento de dados, sejam exigidas pela legislação da UE ou do Estado-Membro a que o subcontratante está sujeito, o subcontratante deve informar o responsável pelo tratamento de dados desse requisito legal antes do processamento, exceto se essa legislação proibir tal informação por razões de interesse público importantes.

a. Sem instruções documentadas do responsável pelo tratamento de dados, o subcontratante não pode, portanto, no âmbito das Cláusulas:

b. transferir dados pessoais para um responsável pelo tratamento de dados ou para um subcontratante num país terceiro ou numa organização internacional;

c. transferir o processamento de dados pessoais para um subcontratante num país terceiro;

d. ter os dados pessoais processados pelo subcontratante num país terceiro.

7.3. As instruções do responsável pelo tratamento de dados relativamente à transferência de dados pessoais para um país terceiro, incluindo, se aplicável, o instrumento de transferência ao abrigo do Capítulo V do RGPD em que se baseiam, devem ser estabelecidas no Apêndice C.6.

7.4. As Cláusulas não devem ser confundidas com as cláusulas-tipo de proteção de dados na aceção do Artigo 46(2)(c) e (d) do RGPD, e as Cláusulas não podem ser invocadas pelas partes como instrumento de transferência ao abrigo do Capítulo V do RGPD.

8. ASSISTÊNCIA AO RESPONSÁVEL PELO TRATAMENTO DE DADOS

8.1. Tendo em conta a natureza do processamento, o subcontratante deve assistir o responsável pelo tratamento de dados por meio de medidas técnicas e organizativas adequadas, na medida em que tal seja possível, no cumprimento das obrigações do responsável pelo tratamento de dados para responder a pedidos de exercício dos direitos do titular dos dados previstos no Capítulo III do RGPD.

Tal implica que o subcontratante deve, na medida em que tal seja possível, assistir o responsável pelo tratamento de dados no cumprimento com:

a. o direito de ser informado aquando da recolha de dados pessoais do titular dos dados;

b. o direito de ser informado quando os dados pessoais não foram obtidos junto do titular dos dados;

c. o direito de acesso pelo titular dos dados;

d. o direito de retificação;

e. o direito ao apagamento ("direito a ser esquecido");

f. o direito à limitação do tratamento;

g. a obrigação de notificação relativamente à retificação ou apagamento de dados pessoais ou à limitação do tratamento;

h. o direito à portabilidade dos dados;

i. o direito de oposição;

j. o direito de não ser sujeito a uma decisão tomada exclusivamente com base em processamento automatizado, incluindo definição de perfis.

8.2. Para além da obrigação do subcontratante de assistir o responsável pelo tratamento de dados ao abrigo da Cláusula 6.3., o subcontratante deve ainda assistir o responsável pelo tratamento de dados no cumprimento com:

a. A obrigação do responsável pelo tratamento de dados de, sem demora injustificada e, sempre que possível, o mais tardar 72 horas após ter tomado conhecimento, notificar a violação de dados pessoais à autoridade de controlo competente, a menos que seja improvável que a violação resulte num risco para os direitos e liberdades das pessoas singulares;

b. a obrigação do responsável pelo tratamento de dados de efetuar uma avaliação do impacto das operações de processamento previstas sobre a proteção de dados pessoais (avaliação de impacto sobre a proteção de dados);

c. a obrigação do responsável pelo tratamento de dados de consultar a autoridade de controlo competente antes do processamento, quando uma avaliação de impacto indicar que o processamento resultaria num risco elevado.

8.3. As partes devem definir no Apêndice C as medidas técnicas e organizativas adequadas pelas quais o subcontratante é obrigado a assistir o responsável pelo tratamento de dados, bem como o âmbito e a extensão da assistência requerida. Tal aplica-se às obrigações previstas nas Cláusulas 9.1. e 9.2.

9. NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS

9.1. Em caso de qualquer violação de dados pessoais, o subcontratante deve, sem demora injustificada após ter tomado conhecimento, notificar o responsável pelo tratamento de dados da violação de dados pessoais.

9.2. A notificação do subcontratante ao responsável pelo tratamento de dados deve, se possível, ocorrer dentro de 24 HORAS após o subcontratante ter tomado conhecimento da violação de dados pessoais, para permitir ao responsável pelo tratamento de dados cumprir a sua obrigação de notificar a violação à autoridade de controlo competente, cf. Artigo 33 do RGPD.

9.3. Em conformidade com a Cláusula 9(2)(a), o subcontratante deve assistir o responsável pelo tratamento de dados na notificação da violação de dados pessoais à autoridade de controlo competente, assistindo na obtenção das seguintes informações:

- a. A natureza dos dados pessoais, incluindo, sempre que possível, as categorias e o número aproximado de titulares dos dados em causa, e as categorias e o número aproximado de registos de dados pessoais em causa;
- b. as prováveis consequências da violação de dados pessoais;
- c. as medidas tomadas ou propostas pelo responsável pelo tratamento para fazer face à violação de dados pessoais, incluindo, se for caso disso, medidas para atenuar os seus possíveis efeitos negativos.

9.4. As partes devem definir no Apêndice C todos os elementos a fornecer pelo subcontratante quando assistir o responsável pelo tratamento de dados na notificação de uma violação de dados pessoais à autoridade de controlo competente.

10. APAGAMENTO E DEVOLUÇÃO DE DADOS

10.1. Aquando da cessação da prestação de serviços de processamento de dados pessoais, o subcontratante fica obrigado a eliminar todos os dados pessoais processados em nome do responsável pelo tratamento de dados e a certificar ao responsável pelo tratamento de dados que o fez, salvo se a legislação da União ou do Estado-Membro exigir o armazenamento dos dados pessoais.

O subcontratante compromete-se a processar os dados pessoais exclusivamente para as finalidades e durante o prazo previsto por esta legislação e nas condições estritas aplicáveis.

11. AUDITORIA E INSPEÇÃO

11.1. O subcontratante deve colocar à disposição do responsável pelo tratamento de dados todas as informações necessárias para demonstrar o cumprimento das obrigações estabelecidas no Artigo 28 e nas Cláusulas, e permitir e contribuir para auditorias, incluindo inspeções, realizadas pelo responsável pelo tratamento de dados ou por outro auditor mandatado pelo responsável pelo tratamento de dados.

11.2. Os procedimentos aplicáveis às auditorias do responsável pelo tratamento de dados, incluindo inspeções, ao subcontratante e subcontratantes são especificados no Apêndice C.7.

11.3. O subcontratante fica obrigado a proporcionar às autoridades de controlo que, nos termos da legislação aplicável, têm acesso às instalações do responsável pelo tratamento de dados e do subcontratante, ou a representantes que atuam em nome de tais autoridades de controlo, acesso às instalações físicas do subcontratante mediante apresentação de identificação adequada.

12. ACORDO DAS PARTES SOBRE OUTROS TERMOS

12.1. As partes podem acordar outras cláusulas relativas à prestação do serviço de processamento de dados pessoais, especificando, por exemplo, responsabilidade, desde que não contradigam direta ou indiretamente as Cláusulas nem prejudiquem os direitos ou liberdades fundamentais do titular dos dados e a proteção conferida pelo RGPD.

13. INÍCIO E CESSAÇÃO

13.1. As Cláusulas produzem efeitos na data de assinatura por ambas as partes.

13.2. Ambas as partes têm o direito de exigir a renegociação das Cláusulas se alterações à legislação ou a ineficácia das Cláusulas derem origem a tal renegociação.

13.3. As Cláusulas aplicam-se durante a duração da prestação de serviços de processamento de dados pessoais. Durante a duração da prestação de serviços de processamento de dados pessoais, as Cláusulas não podem ser rescindidas, salvo se outras Cláusulas que regulam a prestação de serviços de processamento de dados pessoais tiverem sido acordadas entre as partes.

13.4. Se a prestação de serviços de processamento de dados pessoais for rescindida e os dados pessoais forem eliminados ou devolvidos ao responsável pelo tratamento de dados nos termos da Cláusula 11.1. e do Apêndice C.4., as Cláusulas podem ser rescindidas por aviso prévio escrito de qualquer das partes.

14. PONTO DE CONTACTO PARA O RESPONSÁVEL PELA PROTEÇÃO DE DADOS

14.1. O responsável pelo tratamento pode, a qualquer momento, contactar o Responsável pela Proteção de Dados da Tjekvik relativamente ao processamento de dados pessoais realizado pelo subcontratante. O Responsável pela Proteção de Dados pode ser contactado por e-mail: legal@tjekvik.com.

15. ASSINATURA

Em nome do responsável pelo tratamento de dados, o Acordo de Processamento de Dados é aplicado de acordo com os especificadores nos termos e condições.

Em nome do subcontratante

Nome	Christian Mark
Cargo	CEO
Assinatura	

APÊNDICE A — INFORMAÇÃO SOBRE O PROCESSAMENTO

O processamento de dados pessoais pela Tjekvik, o subcontratante, para o Responsável, limita-se a dados ao abrigo do Art. 6.

Os dados pessoais relativos aos clientes do responsável pelo tratamento de dados são eliminados no prazo de 15 dias.

Os dados pessoais relativos aos funcionários do Responsável (nomes, endereços de e-mail e funções de utilizador) são processados pela Tjekvik para garantir que cada utilizador tem o acesso correto ao backend da Tjekvik. Os utilizadores e os seus dados podem ser mantidos diretamente pelo administrador de conta (centralmente em vários workshops) ou pelos gestores de loja. Os dados são armazenados durante o tempo que o responsável pelo tratamento de dados necessitar dos dados.

A.1. FINALIDADE DO PROCESSAMENTO

O produto é uma tecnologia de self-service intuitiva para a indústria automóvel, que permite aos clientes fazer o check-in e check-out como, quando e onde quiserem — em casa, no concessionário através do quiosque interior ou em segurança no exterior através do quiosque exterior. O cliente faz o check-in e check-out com número de telefone ou matrícula.

Os dados são processados para:

- Permitir ao cliente iniciar o check-in antes do início do agendamento marcado
- Permitir ao cliente utilizar o self-service durante o check-in
- Permitir ao cliente utilizar o self-service durante o check-out

A.2. NATUREZA DO PROCESSAMENTO

- Recolha
- Registo
- Organização
- Estruturação
- Armazenamento
- Recuperação
- Utilização
- Alinhamento ou combinação
- Limitação
- Apagamento ou destruição

A.3. TIPOS DE DADOS PESSOAIS

- Nome
- Morada
- E-mail
- Número de telefone
- Matrícula
- Número VIN
- Detalhes sobre o veículo específico (marca, modelo)
- Detalhes do pedido (conteúdo do trabalho planeado e, em alguns casos, preço)

A.4. CATEGORIAS DE TITULARES DE DADOS

- Clientes atuais do workshop do responsável pelo tratamento de dados.
- Funcionários do responsável pelo tratamento de dados.

A.5. DURAÇÃO DO PROCESSAMENTO

A duração de cada processamento para o titular dos dados é geralmente de 9 dias, a partir do momento em que o subcontratante importa os dados de uma API. Após 9 dias, o sistema apaga os dados pessoais.

Em determinadas situações, os dados são processados por um máximo de 15 dias. Tal ocorre quando o subcontratante importa os dados de um sistema CSV, e não de uma solução API.

APÊNDICE B — SUBCONTRATANTES AUTORIZADOS

B.1. SUBCONTRATANTES APROVADOS

No início das Cláusulas, o responsável pelo tratamento de dados autoriza a contratação dos seguintes subcontratantes:

NOME	NIF/CVR	MORADA	DESCRIÇÃO DO PROCESSAMENTO	BASE LEGAL
HEROKU	NIF EUA: 26-1088476 Nº empresa: C3096268	Salesforce/Heroku 415 Mission Street Suite 300 San Francisco, CA 94105	Alojamento em cloud da aplicação Tjekvik (em servidores AWS) AWS DUB2: Dublin, Irlanda AWS FRA54: Frankfurt, Alemanha Dados dos clientes não saem da UE.	EU-U.S. Data Privacy Framework (certificação ao Departamento de Comércio dos EUA).
AMAZON	Nº empresa: C3568304	HQ: 410 Terry Avenue North Seattle, WA 98109-5210	Alojamento em cloud do servidor SFTP para importações via CSV. Região europeia: Dublin, Irlanda e Frankfurt, Alemanha. Dados dos clientes não saem da UE.	EU-U.S. Data Privacy Framework (certificação ao Departamento de Comércio dos EUA).
TWILIO	Nº empresa: 10994798-0143	HQ: 375 Beale Street Suite 300 San Francisco, CA 94105 EUA	Operações de SMS. Servidor nos EUA (região US1).	EU-U.S. Data Privacy Framework (certificação ao Departamento de Comércio dos EUA).
SINCH SWEDEN AB (ou fornecedor escolhido pelo cliente)	556747-5495	Lindhagensgatan 74 112 18 Estocolmo, Suécia	Servidor na UE/EEE: Dublin, Irlanda e Frankfurt, Alemanha.	—
Mailgun	Nº empresa: 0802653513	112 E Pecan St. #1135 San Antonio, TX 78205, EUA	Operações de e-mail. Data center na Alemanha. Dados dos clientes não saem da UE.	Cláusulas Contratuais-Tipo da Comissão Europeia (Decisão 2021/914).

Os subcontratantes americanos da Tjekvik certificaram ao Departamento de Comércio dos EUA que aderem aos Princípios do Quadro de Privacidade de Dados UE-EUA. A Mailgun está abrangida pelas Cláusulas Contratuais-Tipo modernizadas da Comissão Europeia (Decisão de Execução (UE) 2021/914). Todos os dados pessoais processados em nome do responsável são processados no território da UE/EEE.

B.2. AVISO PRÉVIO PARA A AUTORIZAÇÃO DE SUBCONTRATANTES

Se a Tjekvik adicionar um subcontratante, será dado aviso prévio ao responsável pelo tratamento de dados com pelo menos 6 semanas de antecedência. Se o responsável pelo tratamento de dados tiver objeções à alteração, a objeção deve ser feita o mais rapidamente possível e o mais tardar 21 dias após o responsável pelo tratamento de dados ter recebido a notificação. Qualquer alteração é formalizada mediante aditamento assinado por ambas as partes.

APÊNDICE C — INSTRUÇÃO RELATIVA À UTILIZAÇÃO DE DADOS PESSOAIS

C.1. OBJETO/INSTRUÇÃO PARA O PROCESSAMENTO

O subcontratante processa os dados pessoais para fornecer a "Tjekvik, recepção digital de serviços" ao responsável pelo tratamento de dados em conformidade com os Termos de Serviço. Os dados que a Tjekvik recolhe são provenientes do sistema DMS ou API do Responsável. Em casos raros, os dados são recolhidos junto do titular dos dados — o que garante o direito de retificação e que os dados processados estão corretos.

C.2. SEGURANÇA DO PROCESSAMENTO

O processamento envolve dados ao abrigo do Artigo 6 do Regulamento. Não são processados dados ao abrigo dos Artigos 9 ou 10. Existe um baixo risco de violação dos direitos e liberdades do titular dos dados.

C.2.1. A proteção de dados é gerida pelo CTO e pelo Responsável Jurídico. A Tjekvik forma os funcionários na proteção de dados pessoais dentro da organização.

C.2.2. Criptografia: A Tjekvik utiliza HTTPS por defeito entre uma API e para contas de utilizadores. As palavras-passe dos utilizadores são encriptadas na base de dados. O conteúdo transmitido pela rede é sempre transmitido via HTTPS com certificado de chave pública de 2048 bits. O SSLv3 e versões anteriores, bem como o TLS 1.0, estão desativados. Quando os dados são transferidos entre sistemas, são encriptados em trânsito (SFTP/HTTPS); existe a opção para os concessionários adquirirem criptografia adicional (dados encriptados em repouso).

C.2.3. Confidencialidade, integridade e disponibilidade: A Tjekvik possibilitou que os titulares dos dados retifiquem informações de contacto. Os administradores de loja e de conta podem adicionar, retificar ou eliminar informações. É realizado um backup completo dos dados a cada 6 horas, com backups delta entre eles.

C.2.4. Recuperação de dados: A Tjekvik armazena apenas uma quantidade muito limitada de dados por um período muito limitado. Se necessário, devido a um evento físico ou técnico, os dados perdidos podem ser reimportados e disponibilizados novamente.

C.2.5. Testes regulares: É realizado um teste de penetração de forma recorrente. Todos os funcionários são instruídos nas diretrizes relativas ao processamento de dados pessoais.

C.2.6. Gestão de Acessos

Controlo de Acesso Físico: A Tjekvik é uma empresa totalmente remota. Nenhuma infraestrutura está alojada num escritório ou instalação. A plataforma é baseada na cloud e todas as políticas de controlo de acesso físico são geridas pela Heroku e pela AWS.

Controlo de Acesso ao Sistema: O acesso a recursos digitais é limitado às pessoas que deles necessitam: principalmente suporte de 1.º e 2.º nível e equipa de DevOps. A segurança é garantida através da utilização de chaves SSH e login de utilizador com política de palavras-passe fortes e/ou MFA.

Controlo de Acesso aos Dados: O acesso a recursos de dados é limitado às pessoas que deles necessitam: suporte de 2.º nível apenas em modo de leitura em produção. A segurança é garantida através da utilização de chaves SSH e login de utilizador com política de palavras-passe fortes e/ou MFA.

Controlo de Transmissão de Dados: O conteúdo transmitido pela rede é sempre transmitido via HTTPS com certificado de chave pública de 2048 bits. O SSLv3 e versões anteriores, bem como o TLS 1.0, estão desativados.

Controlo de Entrada: Os dados importados de sistemas externos são verificados quanto a consistência e ataques de injeção SQL. Um teste de penetração (operado pela empresa Sapphire) foi realizado em 05/2022. Não foi detetado nenhum problema CRÍTICO; todos os problemas de nível ALTO foram resolvidos no 3.º trimestre de 2022. Os testes de penetração serão organizados de 2 em 2 anos.

Controlo de Disponibilidade: Existe um sistema de alertas caso a plataforma fique inoperacional (todos os componentes são monitorizados e geram alertas separadamente). A failover e redundância serão implementadas após a migração completa da infraestrutura para AWS.

C.3. ASSISTÊNCIA AO RESPONSÁVEL PELO TRATAMENTO DE DADOS

A Tjekvik notificará o responsável pelo tratamento de dados, se possível, no prazo de 24 HORAS após ter tomado conhecimento da violação de dados pessoais, para permitir ao responsável pelo tratamento de dados cumprir a sua obrigação de notificação ao abrigo do Artigo 33 do RGPD.

C.4. PERÍODO DE ARMAZENAMENTO/PROCEDIMENTOS DE APAGAMENTO

O período geral de armazenamento é de 14 dias. Se um titular dos dados ainda não tiver levantado a chave do veículo, os seus dados não serão eliminados antes do levantamento da chave. O período pode ser alargado até 25 dias se a fonte de importação de agendamentos for um ficheiro CSV, para garantir a disponibilidade para checkout.

C.5. LOCAL DE PROCESSAMENTO

O processamento dos dados pessoais ao abrigo das Cláusulas será realizado nos locais indicados em B.1. e nas instalações da Tjekvik.

C.6. INSTRUÇÃO SOBRE A TRANSFERÊNCIA DE DADOS PESSOAIS PARA PAÍSES TERCEIROS

Todas as transferências para países terceiros têm base legal de transferência. No que diz respeito a transferências para países terceiros não considerados seguros, a Tjekvik acompanhará de forma contínua e pelo menos anualmente se o subcontratante ainda cumpre os requisitos de segurança estabelecidos no RGPD. Caso os requisitos não sejam cumpridos, a Tjekvik encerrará imediatamente a cooperação com o subcontratante e informará o Responsável, utilizando o procedimento acordado estabelecido em B.2.

C.7. PROCEDIMENTOS PARA AUDITORIAS DO RESPONSÁVEL PELO TRATAMENTO DE DADOS

O responsável pelo tratamento de dados ou o seu representante tem direito a realizar uma inspeção física anual dos locais onde o processamento de dados pessoais é realizado pelo subcontratante, incluindo instalações físicas e sistemas utilizados para e relacionados com o processamento, para verificar a conformidade com o RGPD, as disposições aplicáveis de proteção de dados da UE ou do Estado-Membro e as Cláusulas. Para além da inspeção planeada, o responsável pelo tratamento de dados pode realizar uma inspeção ao subcontratante quando o considerar necessário.