Privacy Policy for your customer account, the app and online ordering

As of: 4 November 2026

This is a translation for convenience. The German version is binding; where this translation is more favourable to you, it applies.

New in this version: In the app from version 1.1.0 and in the order portal, before we send you a code, we have Cloudflare Turnstile check whether the request comes from a human; Cloudflare also uses this information itself to improve the check, and Google also receives your IP address in the process. In the order portal, Cloudflare stores an entry and a small file in your browser for this purpose, which remain without an expiry date; Cloudflare can use the entry to recognise your browser in later checks (sections 11.7 and 12.4). We now only send a limited number of text messages with codes and only to mobile numbers from the EU and Switzerland (sections 11.7 and 11.8). We send e-mails with codes and booking confirmations through the e-mail service Resend, which stores them in the USA for 30 days (sections 3.2, 5.3 and 15.1). If you order to take away, we store this with your booking, and if you withdraw from the contract for drinks or sauces, we store your statement and send you an acknowledgement of receipt (sections 5.1 and 5.3). Replies to our e-mails about your bookings go to our mailbox kontakt@citychicken-nhas.de, and we also handle them for the operating company (sections 2.4 and 5.3). If the staff at the door change the type of your order at your request, we store this (sections 5.1 and 5.7). Before your ticket expires, we remind you by e-mail that it is about to expire, and if our system then cancels your booking, we let you know (section 5.3).

In this Privacy Policy, you will find out which personal data is processed when you use the “Nhas City Chicken” app for iOS or Android or the order portal on our website at citychickennhas.de/bestellen (the “order portal”), above all for your customer account and your bookings. Together, the app and the order portal are called the “platform”; you use both with the same customer account. Where something only applies to the app or only to the order portal, we say so expressly. You will also find out who is responsible for the processing, for what purposes and on what legal basis the data is processed, how long it is stored and what rights you have. “We” means Nhas Food 1993 GmbH.

The other pages of our website citychickennhas.de are covered by their own privacy policy, which describes in particular the website’s cookie banner and the analytics and advertising services that we use only on those pages and only with your consent. This Privacy Policy is available in German and English; if you choose a language other than German in the order portal, the links lead to the English version.

1. Key points at a glance

1.1 Overview

- The app and the order portal are operated by Nhas Food 1993 GmbH. Each “City Chicken” restaurant is run by its own company, the operating company; in Cologne, this is MOG Gastro GmbH. You make the contract for your booking with this company, whether you book in the app or in the order portal, and we take care of your booking together with it. You can contact us with any questions about data protection.
- We use your data for your customer account, your bookings, your requests and the security of the app and the order portal. We do not sell it.
- When you check in at the restaurant, we pass your order with your first name to the restaurant’s point-of-sale system so that the kitchen can prepare it and the till can record it. It remains stored there for as

long as the operating company has to keep its till records, usually ten years, even if you delete your customer account (section 5.7). We then show you the till receipt in the app and in the order portal (section 5.8).

- The app does not show advertising from other companies, does not read any advertising identifier and does not analyse how you use it. In the order portal, we do not use any analytics or advertising services; your browser only stores there what is needed for the functions you use and, during the check before a code, also an entry and a file from Cloudflare that remain after the check without an expiry date (section 12.4). However, Stripe's payment module, in the app Google's services for push notifications and the map, and in older app versions also for checking the internet connection, on the iPhone Apple's map, and before a code the check by Cloudflare Turnstile collect technical data about your device or browser themselves, Turnstile also on how the check is operated (sections 6 to 8, 11.7 and 12.6).
- The app only loads the map showing the restaurants if you agree and confirm that you are at least 16 years old (section 8).
- We do not receive your precise location. Cloudflare derives an approximate location from your IP address, such as the city and postcode, which remains in the logs of our interface for no more than 7 days (section 11.9).
- You can delete your customer account in the app and in the order portal, export your data there, ask for information about your data and complain to a data protection authority (section 17).

Your right to object: Where we process data on the basis of legitimate interests (Art. 6(1)(f) GDPR), you have the right to object, on grounds relating to your particular situation, at any time to this processing. You can find the details in section 17.

2. Who is responsible?

2.1 Nhas Food 1993 GmbH

The app and the order portal are operated by Nhas Food 1993 GmbH, Südwestkorso 14, 12161 Berlin, represented by its managing director, Nesrin Nhas, e-mail media@citychicken-nhas.de, phone +49 30 62904952. We alone are responsible for registration and sign-in, your customer account and your profile, push notifications, the restaurant map, the contact form, protection against misuse, showing that you are signed in in the header of our website (section 13.2) and the addresses at nhascitychicken.app (section 13.1).

2.2 Operating companies of the restaurants

Each "City Chicken" restaurant is operated by its own company (the operating company), with which you conclude the booking contract. The restaurant in Cologne, Breite Straße 29, is operated by MOG Gastro GmbH, Torstraße 125, 10119 Berlin, represented by its managing director, Adel Khalaf, e-mail mog@citychicken1993.de, phone +49 1525 7378706. If another restaurant becomes bookable in the app or in the order portal, we name its operating company here before you can book there.

2.3 Joint responsibility for bookings

We and the operating company of the booked restaurant are jointly responsible (Art. 26 GDPR) for the hold, the booking, the order and the payment, for the QR ticket and the check-in, including passing your order to the restaurant's point-of-sale system and the status reported back, for providing your till receipt, for cancellations, withdrawals and refunds, for the booking confirmation, for ratings of your visit and for your requests about a booking, including after your visit. This applies equally to bookings in the app and

in the order portal. The operating company uses your booking data to serve you, to receive your payment and to reach you if anything changes, and your rating to improve its restaurant. Other operating companies do not receive your booking. The operating company alone is responsible for the data in its point-of-sale system (section 5.7).

2.4 The essence of our arrangement

In an arrangement under Art. 26 GDPR, we and the operating company have set out who fulfils which obligation:

- We inform you and are your central point of contact for all data protection matters. The operating company forwards any requests it receives to us without undue delay.
- We operate and secure the app, the order portal and the systems behind them, decide which data is collected and what your device or browser stores for this, and conclude the contracts with the technical service providers. The operating company concludes the contracts with Stripe and with the provider of its point-of-sale system itself and also decides which payment methods it offers.
- At check-in, we pass your order to the operating company's point-of-sale system. We decide together which data goes there. In the point-of-sale system, the operating company decides who has access to your data, how long it is kept and when it is deleted; it provides information about this data through us. In your customer account, we provide you, on behalf of the operating company, with the till receipt that the point-of-sale system sends us.
- We only collect and store ratings of your visit so that the operating company can improve its restaurant; we do not use them for our own purposes.
- Replies to our e-mails about your booking go to our mailbox kontakt@citychicken-nhas.de. We also handle them for the operating company and pass on to it what it needs for your booking, such as a statement about a refund or a return.
- The operating company only gives access to your booking to the staff who need it and obliges them to keep it confidential.
- The companies inform each other of data breaches without undue delay. We report incidents involving the app, the order portal or our systems to the supervisory authority and tell you about them if the law requires this; the operating company deals with incidents in the restaurant.

Even so, you can exercise your rights against each of the companies involved.

2.5 After your booking is completed

We show you your bookings in your customer account for as long as it exists; we alone are responsible for this. After your visit or a cancellation, the operating company alone is responsible insofar as it stores booking and payment data because the law requires it to keep this data, and uses the data for its accounting (Art. 6(1)(c) GDPR), or asserts or defends claims under the booking contract (Art. 6(1)(f) GDPR; its legitimate interest is to resolve such claims). In doing so, we act only on its behalf and on its instructions.

2.6 Data protection officer

Nhas Food 1993 GmbH and MOG Gastro GmbH have appointed the same data protection officer. You can reach him at the address of Nhas Food 1993 GmbH, marked "Datenschutzbeauftragter" (data protection officer), or by e-mail to r.heyne@citychicken-nhas.de.

3. Registration, sign-in and customer account

3.1 Which data

You need a customer account to book in the app or in the order portal. The same account works for both, and you sign in to the app and the order portal with the same details. For this, we process:

- your e-mail address,
- your first and last name,
- your mobile number,
- in the app, your country,
- the language of your customer account, German or English; in the app, you choose it yourself, and in the order portal we take German when you register if you use the pages in German, and English otherwise,
- the time and version of your agreement to the Terms and Conditions, the version of this Privacy Policy that we pointed you to at that time, and the time at which you took note of a new version, each with the kind of event and, where the app or the order portal sends them, the channel (app for iOS or Android, or order portal), its version, the language of the text and of the screen, the identifier of the wording shown and the checksum of the text.

Your e-mail address, name and mobile number are required, and in the app also your country; without them, you cannot create a customer account or book. A profile picture and, in the app, links are optional (section 4).

3.2 Sign-in with codes

There is no password. When you register, you receive a code by e-mail, and you confirm your mobile number with a code sent by text message (SMS). After that, you sign in with a code sent by text message; as long as your number has not been confirmed, you receive the code by e-mail. Supabase manages the customer accounts for us. A function at Supabase passes the text messages to Twilio, which sends them; we only send text messages to mobile numbers from a member state of the European Union or from Switzerland (section 11.8). The e-mails with codes are created by a function at Supabase and sent via the e-mail service Resend (section 14.1), and replies to them reach our mailbox kontakt@citychicken-nhas.de. If your e-mail address looks like a typo, has an ending that does not exist or belongs to a service for disposable addresses, we do not send a code and tell you so; if an unusually large number of codes is currently going to addresses at the same e-mail provider, we temporarily do not send one. In the app from version 1.1.0 and in the order portal, we also have a check carried out before a code to see whether the request comes from a human (section 11.7).

In the order portal, your browser connects directly to Supabase for the codes sent by e-mail and for confirming your mobile number, just like the app. Before that, your browser sends the proof of the check before a code (section 11.7) to our server at Vercel (section 11.5), which obtains the approval for the code from our interface. If you sign in there with a code sent by text message, our server at Vercel (section 11.5) checks the code through our interface. Our server then stores your sign-in in a cookie in your browser (section 12.4). When you sign in or register, you can tick the box “Stay signed in”. If you do not tick it, your sign-in ends when you close your browser, unless your browser restores your last session. If you tick it, you remain signed in until you sign out or have not used the order portal for 30 days.

3.3 Legal basis

The legal basis is Art. 6(1)(b) GDPR, because the processing is necessary for the user agreement for the platform, that is, for your customer account in the app and the order portal. We need your confirmed mobile number so that the restaurant can reach you if anything changes and so that nobody blocks time slots with many customer accounts. We store the record of your agreement to the Terms and Conditions so

that we can prove that the contract was concluded; to that extent, the legal basis is also our legitimate interest in keeping this record (Art. 6(1)(f) GDPR). When you sign in, we also process your IP address to detect and fend off misuse (section 11). We base the check of your e-mail address before a code and the limits per e-mail provider (section 3.2) on our legitimate interest in delivering codes reliably, protecting our sender address from being blocked by e-mail providers and fending off customer accounts created in bulk with disposable addresses (Art. 6(1)(f) GDPR).

4. Optional profile details

4.1 Profile picture and links

In your profile, you can choose to add a profile picture and, in the app, links to your Instagram or TikTok profile. We show these details to you in the app and the order portal and, as long as you are signed in to the order portal, also show your profile picture or your initials in the header of our website (section 13.2); we do not use them for anything else. Other users do not see your profile details; on our side, only authorised persons can see them.

The app only accesses your camera and photo library when you start this yourself; if your device requires permission for this, it asks you first. From your photo library, the app only takes the picture you select. In the order portal, you select the picture through your browser's file dialog and choose the section to use. Our server at Vercel (section 11.5) checks the picture, removes metadata such as the location, time and camera details, reduces it to no more than 1024 × 1024 pixels and stores only this cleaned picture with our service provider Supabase.

4.2 Legal basis and changes

The legal basis is Art. 6(1)(b) GDPR, because the profile is a function of the user agreement that you can choose to use. You can change your name in the app and in the order portal, and your links in the app. You can replace a profile picture in the app, and replace or remove it in the order portal; if you want to remove it in the app, write to us at media@citychicken-nhas.de. When a profile picture is replaced or removed, we delete the previous file immediately. If, after a new picture has been uploaded, it cannot be added to your profile, the uploaded file remains stored until your customer account is deleted (section 16.1).

5. Booking, order and check-in

5.1 Which data

When you book a time slot, we process the following together with the operating company (section 2.3):

- the restaurant, the number of people, the time slot and whether you eat in or order to take away, including during the hold while you order,
- the food and drinks ordered with your choices, and prices and taxes,
- the payment status and Stripe's payment reference,
- the time at which you confirmed the rules on cancellation and check-in, with the check-in window, the deadline for free cancellation, the refund share and the version of the Terms and Conditions that apply to your booking,
- your QR ticket with the booking code and the day until which it is valid, the time of your check-in and the person who checked you in and, if the staff at the door do not let you in, the time of that decision and the person who made it, as well as, if they change the type of your order there at your request, the new type, the time and the person who changed it,

- after check-in, your pickup number, the status of your order in the point-of-sale system, a copy of the receipt data, the till receipt as a PDF file and, where applicable, the refund of a difference (sections 5.7 and 5.8),
- where applicable, cancellations, withdrawals with their content, the channel and the time they were received, after a withdrawal whether and when you returned the items or proved that you sent them and whether they came back opened, and refunds.

A booking is not possible without these details. In the order portal, your browser stores your basket until you order, for no more than seven days (section 12.4).

5.2 Who can see the booking

On the business day of your time slot, the staff at the restaurant's door can see the following in a list of bookings, even before you check in:

- your first name and the first letter of your last name,
- the number of people, the time slot and whether you eat in or order to take away,
- your order with the total amount and our order number,
- the status of your booking, for example whether you have checked in, and after check-in the status of your order in the point-of-sale system and your pickup number.

If you show your ticket on a later day, the staff at the door see these details as soon as they scan your ticket or enter your booking code, and after your check-in also in that day's list.

After check-in, the staff at the till and the kitchen see your first name, your order, our order number, the time slot, the number of people, your pickup number and whether you ordered to take away, on the kitchen screen or on a kitchen ticket. The staff at the door can then also open your till receipt in order to reconcile it with the till and to clarify queries (section 5.8).

Authorised persons at the operating company and in our administration see bookings with your name and contact details, insofar as they need them for running the restaurant, for queries, refunds and accounting. If someone opens or edits bookings or other guest data in our management system, for example when checking you in at the door, we record who opened or edited which bookings or customer accounts, when, and what was changed. Our legitimate interest in this is being able to trace who has accessed your data and to investigate unauthorised or improper access (Art. 6(1)(f) GDPR). We delete these records after one year, unless we need individual records for longer to investigate a specific incident.

5.3 Booking confirmation by e-mail

After your booking, you receive a booking confirmation by e-mail. We send it in the name of the operating company via the e-mail service Resend and, if Resend is disrupted, via Cloudflare's e-mail service; replies go to our mailbox kontakt@citychicken-nhas.de, and we also handle them for the operating company (section 2.4). We use the same route to remind you before your ticket expires and to let you know when our system cancels your booking after it has expired, when the restaurant cancels your booking or when we refund a difference because the till charged less than you paid (section 5.7). If you withdraw from an order to take away in the app or in the order portal via "Withdraw from contract", we also send you the acknowledgement of receipt this way, to the e-mail address you give there, and later, to the same address, the message whether the restaurant refunds the items you returned; if you withdraw after check-in, we also tell the restaurant about it with the order number, time slot and items, without your name or contact details. If you declare a withdrawal by e-mail, by letter, by phone or at the counter, the staff record it with the way it came in and the time it was received, and we send you the acknowledgement of receipt to the address your e-mail came from or otherwise to the address of your customer account. If a reply to these e-

mails does not concern your booking or contains information about health problems, we process it like a message sent through the contact form (sections 10.1 and 10.2); it remains stored in our mailbox (section 16.1).

5.4 No note on your order

You cannot add a note for the restaurant to your order, so we do not pass any note on to the point-of-sale system either. Please raise allergies and intolerances directly at check-in.

5.5 Rating of your visit

Once the restaurant has marked your booking as completed, the app asks you on the home screen to rate your visit; the order portal does not ask for ratings. It is up to you whether you do so; if you do, you give stars and can add a comment. The rating belongs to your booking: the operating company uses it to improve the food and service in its restaurant. For this purpose, we collect and store it within our joint responsibility for your booking (section 2.3) with your order, your customer number and the time, and we do not use it for our own purposes. Authorised persons at the operating company and in our administration see it with your first name; other users do not see it. The legal basis is the operating company's legitimate interest in improving its restaurant (Art. 6(1)(f) GDPR). We delete the rating together with your customer account (section 16.1).

5.6 Legal basis

The legal basis is Art. 6(1)(b) GDPR, because the processing is necessary for your booking contract with the operating company and for your user agreement with us. The booking confirmation and the acknowledgement of receipt of a withdrawal are also required by law (Art. 6(1)(c) GDPR in conjunction with § 312f Abs. 2 and § 356a Abs. 4 BGB (German Civil Code)). Section 16 explains how long booking and payment data is kept. Section 5.7 applies to passing your order to the restaurant's point-of-sale system.

5.7 Passing your order to the restaurant's point-of-sale system

When you check in at the restaurant, our server passes your paid order to the operating company's point-of-sale system (Lightspeed Restaurant). This way, the kitchen receives your order on its screen or as a kitchen ticket, and the till records it as paid and creates the till receipt. For this, we transmit:

- your first name, or the word "Gast" (German for "guest") if there is no first name,
- the food and drinks ordered with item number, quantity and your choices; if an item is now more expensive at the till than what you paid, a discount equal to the difference,
- the amount charged by the till, marked as paid through the platform,
- a pickup number under which the restaurant calls your order,
- an order note with our order number, the time slot and the number of people,
- the type of your order, after a change at the door the new one, so that the kitchen knows whether to pack it to take away and the till records it correctly,
- instead of your e-mail address, an e-mail address of ours to which the point-of-sale system sends the till receipt (section 5.8).

We do not transmit your last name, your e-mail address, your mobile number, your customer number or payment data such as Stripe's payment reference. For bookings that you paid for before 6 a.m. on 4 October 2026, we only transmit the word "Gast" instead of your first name. If the transfer fails, the staff enter your order at the till.

If the till charges less for your order than you paid, we automatically refund the difference to your payment method through Stripe on behalf of the operating company and let you know by e-mail (section 5.3).

The point-of-sale system tells us the status of your order, for example whether it has been accepted, is ready or has been cancelled at the till, together with the identifier of the transaction in the till. Once the transaction has been completed, we retrieve the receipt data, and the point-of-sale system sends us the till receipt (section 5.8). With your booking, we store, in addition to the till receipt, the status with the times, the pickup number, the identifier of the transaction in the till, a copy of the receipt data with the receipt number, times, till device, items, taxes and payments without the names of guests or staff, and the result of our price check between the app and the till. This way, the staff at the door can see whether your order has reached the till, and your booking, your payment and the till entry can be matched.

The operating company alone is responsible for your data in the point-of-sale system; Lightspeed processes it there as its processor (sections 14.1 and 15.3). The till records your order and protects the record with its technical security device. The operating company must keep the record and must not alter it in a way that means its original content can no longer be determined (§ 146 Abs. 4 and § 147 AO (German Fiscal Code)). The record therefore remains stored in the point-of-sale system together with your first name even if you delete your customer account; your right to erasure does not apply to this extent (Art. 17(3)(b) GDPR). After your visit, the operating company only uses the record for its accounting and for audits by the tax office; once the retention period has ended, it has it deleted (section 16.1).

The legal basis for passing on your order is Art. 6(1)(b) GDPR, because the restaurant needs your order to fulfil your booking contract. We transmit your first name so that the kitchen and the till can match your order to you; tax law does not require it, but it becomes part of the record. When the operating company records an order with its electronic till, the till must record it individually and protect it with its technical security device; the operating company must issue a receipt for it and keep the records (Art. 6(1)(c) GDPR in conjunction with §§ 146, 146a and 147 AO). We also store the pickup number and the till's receipt number with your booking on behalf of the operating company (section 2.5), because it must be possible to trace how each order came about and how it was handled (Art. 6(1)(c) GDPR in conjunction with § 145 Abs. 1 Satz 2 AO). We store the status of your order, the other receipt data and the price check because we need them for your check-in and to handle your booking, for example for queries and refunds, including the refund of a difference (Art. 6(1)(b) GDPR).

5.8 Till receipt in the app and in the order portal

Once your transaction has been completed at the till, the point-of-sale system sends us the operating company's till receipt as a PDF file to the e-mail address that we transmitted instead of yours (section 5.7). Lightspeed sends it through its e-mail service provider in the USA, currently SendGrid (section 15.3). Cloudflare receives the e-mail for us in its worldwide network (section 15.1) and stores it in a storage facility in the European Union. Our server checks that it comes from Lightspeed, automatically reads the receipt number, the total, our order number and the details of the technical security device from the PDF file and uses them to match the till receipt to your booking. We store the PDF file with these details and a checksum with our service provider Supabase and then delete the e-mail (section 16.1). We delete till receipts for a refund made at the till immediately, without storing them or showing them to you.

After check-in, you can see the till receipt and your pickup number with your booking in the app and in the order portal. If the staff enter your order at the till (section 5.7), the point-of-sale system does not send us a till receipt; you then get it at the till. You can share or save the PDF file; we do not send you the till receipt by e-mail. It contains the details of the till receipt, including the details of the technical security device, as well as your first name, your pickup number and our order number. You can get a paper receipt

at the till on request. The staff at the door can also see your till receipt after check-in in order to reconcile it with the till and to clarify queries (section 5.2).

The legal basis is Art. 6(1)(c) GDPR in conjunction with § 146a Abs. 2 AO, because the operating company must provide you with a receipt, and Art. 6(1)(b) GDPR, because we show you the till receipt in your customer account. We store the till receipt and the related details until your customer account is deleted (section 16.1); until then, you can open and save it with your booking, and your data export shows its number (section 16.2). We and the operating company are jointly responsible for providing the till receipt after your check-in (section 2.3); after that, we show it to you in your customer account under our own responsibility (section 2.5).

6. Payment through Stripe

6.1 How payment works

You pay in advance to the operating company, which has its own account with Stripe for this purpose (Stripe Payments Europe, Limited, Dublin, Ireland). In the app, you pay by credit or debit card or, depending on your device and on activation, with Apple Pay, Google Pay, Klarna or Link; in the order portal, by credit or debit card, with Klarna and, depending on your device and browser, with Apple Pay or Google Pay (section 6.4). You enter your payment details directly in Stripe's payment window in the app, in Stripe's payment field on the checkout page of the order portal or with the payment service you choose; we and the operating company do not receive them. Depending on the payment method, the payment window or the payment field may also ask for your e-mail address, phone number or address; this information goes directly to Stripe or to the service you choose. On behalf of the operating company, we send Stripe the amount, the currency, the order number, the internal identifier of the order, the subtotal, the tax amount, the time slot and the number of people, and in the case of a refund the payment reference, the refund amount, the order number, the internal identifier of the order and the reason for the refund, but neither your name nor your e-mail address. Stripe sends us information about each payment and refund, such as the payment status, the payment reference, the amounts and the payment method, where applicable also features of your payment method such as the card brand and the last four digits of the card number, and information you entered in the payment window or payment field. Of this, we only store the status, the payment reference, the amounts and the payment method without the card number, for example "Visa", "Apple Pay" or "Klarna"; the booking confirmation also shows you the payment method.

If a refund cannot be made through Stripe, the operating company refunds the amount to you another way that we agree with you on its behalf beforehand, for example by bank transfer or in cash at the restaurant; to do so, we write to you by e-mail and keep a copy in our mailbox. For a bank transfer, it only uses the bank details you give us for that purpose; its bank receives your name, your bank details, the amount and the order number. If it pays you the amount in cash, you confirm receipt by signing a receipt. We store how and when the refund was made, and when we wrote to you about it, with your booking (section 5.1); the operating company keeps the record of the bank transfer and the signed receipt as accounting vouchers (section 16.1). The legal basis is Art. 6(1)(b) GDPR, and for a refund after a withdrawal also Art. 6(1)(c) GDPR in conjunction with § 357 Abs. 1 and 3 BGB.

6.2 Data that Stripe collects on your device in the app

Stripe's payment module is part of the app; from version 1.0.3, the app only loads and starts it when you pay, while older versions start it when the app starts. It reads information about your device, such as the device model, operating system, language setting and screen size, as well as an identifier that your device assigns separately for each app provider (on iPhones, the "identifier for vendor"; on Android, the Android ID). In addition, it stores its own identifiers on your device, records how you use the payment window and sends this data to Stripe, including the device identifier, which it also sends together with usage data for

analytics. Stripe uses the data under its own responsibility to detect fraud, to secure the payment window and to improve its products through its own analytics, but, according to Stripe, not for advertising. Stripe decides how long it stores its identifiers on your device; you can find the details in Stripe's privacy policy (section 6.3).

The legal basis for storing and reading this information is § 25 Abs. 2 Nr. 2 TDDDG (German Telecommunications Digital Services Data Protection Act), because this is necessary so that the app's payment function is available securely and fraud can be detected. For the app's transmission of this data to Stripe and for our provision of payment data to Stripe for fraud prevention, we and the operating company rely on the legitimate interest in secure payments and in preventing fraud (Art. 6(1)(f) GDPR).

6.3 Legal basis and role of Stripe

The legal basis for the payment is Art. 6(1)(b) GDPR. Stripe Payments Europe, Limited processes the payment data as a processor on behalf of the operating company. As authorised payment service providers, Stripe Technology Company, Limited, Stripe Payments Europe, Limited and Stripe Technology Europe, Limited, all in Ireland, are jointly responsible in their own right for the payment. Stripe is also responsible in its own right for fraud prevention, for legal obligations such as preventing money laundering and for its own analytics; in the process, data is also sent to Stripe, LLC in the USA (section 15). You can find more information in Stripe's privacy policy; you can also exercise your rights directly with Stripe.

6.4 Apple Pay, Google Pay, Klarna and Link

If you choose Apple Pay or Google Pay, Apple (Apple Distribution International Limited, Cork, Ireland) or Google (Google Ireland Limited, Dublin, Ireland) processes the payment with the payment method from your wallet under its own responsibility. If you choose Klarna, the payment window or the payment field takes you to Klarna (Klarna Bank AB (publ), Sveavägen 46, 111 34 Stockholm, Sweden); Klarna processes the information you provide there, such as your name, address, e-mail address and phone number, under its own responsibility and, according to Klarna, may check your identity and your ability to pay. If you use Link, you give Stripe your e-mail address or phone number yourself, and Stripe stores your payment details in your Link account under its own responsibility. We only offer Link in the app. Klarna's privacy terms apply on Klarna's page, including to cookies that Klarna sets there; in the order portal, you then return to the page of your order (section 12.4). From all of these services, we and the operating company only receive, via Stripe, the information listed in section 6.1. The legal basis is Art. 6(1)(b) GDPR. You can find more information in the privacy policies of Apple, Google, Klarna and Link.

6.5 Data that Stripe collects in your browser in the order portal

In the order portal, we only load Stripe's payment module (Stripe.js) on the checkout page, that is, only once you go to the checkout; the page on which you pay for an order that has not yet been paid also counts as the checkout page. It displays the payment field and helps prevent fraud. For this purpose, it sets the cookies __stripe_mid, with a lifetime of one year, and __stripe_sid, with a lifetime of 30 minutes, for our entire domain citychickennhas.de; both lifetimes start again as soon as Stripe.js is loaded again. According to Stripe, the cookie m, with a lifetime of up to two years, is added for the domain m.stripe.com. Stripe.js also collects characteristics of your browser and device, such as the browser, operating system, language setting and screen size, the address and title of the checkout page, and information on how you use the checkout page and the payment field, such as mouse movements and the time spent, and sends this data to Stripe. According to Stripe, a security check by the hCaptcha service, which Intuition Machines, Inc., USA, operates as a processor for Stripe, may be loaded in the process. According to Stripe, it uses this data only to detect fraud and to secure payments and not for advertising. We and the operating company are jointly responsible for embedding Stripe.js on the checkout page and for transferring this data to Stripe; Stripe is responsible for its further use (section 6.3).

The legal basis for storing and reading this information is § 25 Abs. 2 Nr. 2 TDDDG, because this is necessary so that the payment function you use by opening the checkout is available securely and fraud can be detected. For the transfer to Stripe, we and the operating company rely on the legitimate interest in secure payments and in preventing fraud (Art. 6(1)(f) GDPR).

7. Push notifications

7.1 Permission and device token

As soon as you have registered and confirmed your mobile number, the app asks you whether it may send you notifications; on iPhones and from Android 13 onwards, this happens through your device's dialog. On devices with Android up to version 12, there is no such request; there, notifications are allowed until you turn them off in your device settings. For delivery, Google's notification service Firebase Cloud Messaging creates an installation ID and a device token on your device; this may already happen the first time you start the app. The app sends the token to us, and we store it with your customer account. On iPhones, Apple delivers the notifications through the Apple Push Notification Service. We do not send push notifications in the order portal.

7.2 Which notifications

By push notification, we may send you messages about your bookings and about using the app, for example a notice about a booking or about a change to the app. We do not send you advertising or requests for ratings by push notification; if we want to do so in the future, we will ask you separately beforehand. Notifications may also appear in the app's list of notifications.

7.3 Legal basis and turning them off

The installation ID and the token are stored and read because this is necessary to deliver the notifications (§ 25 Abs. 2 Nr. 2 TDDDG); we base any further processing on Art. 6(1)(b) GDPR. You can turn off the notifications at any time in your device settings. If you sign out, we delete the token on our systems, and from version 1.0.3 the app also has it deleted at Google; if you delete your customer account, we delete it after 30 days at the latest (section 16.1). The installation ID remains on your device until you delete the app; on the iPhone, it may remain in the keychain after that.

8. Restaurant map and location

8.1 Map services from Google and Apple

On Android devices, the map on the app's "Stores" screen comes from Google Maps. On the iPhone, you choose in the notice about the map whether the app loads it from Apple (Apple Maps) or from Google Maps. The app only loads a map when you tap "I am 16 or older – load map" in the notice about the map on Android, or "Load Apple Maps" or "Load Google Maps" on the iPhone; only then does your device connect to the map service you chose. The order portal does not show a map.

If you load the map from Google, according to Google, it processes, among other things, your IP address, device identifiers and usage, performance and crash data, including for its own purposes, and may transfer data to Google LLC in the USA (section 15). We are responsible for embedding the map and for transferring this data to Google, and Google Ireland Limited, Dublin, Ireland, is responsible for its further use; you can find more information in Google's privacy policy.

If you load the map from Apple, your iPhone retrieves the map data from Apple's servers. Apple receives your IP address and, according to its information on Apple Maps, among other things the time of the request, the device model and software version, the input language, the map area visible on your device and details of how you use the map. According to Apple, it associates this usage data with an identifier

that changes several times an hour and is not linked to your Apple Account; for performance, statistics and protecting the service, Apple also uses longer-lived identifiers, which are not linked to your Apple Account either. Apple also uses the data to provide and improve its maps and other location-based services, generally stores data with Apple Inc. in the USA and bases the transfer there on standard contractual clauses. We are responsible for embedding the map and for transferring this data to Apple, and Apple Distribution International Limited, Cork, Ireland, is responsible for its further use; you can find more information in Apple Maps & Privacy and in Apple's privacy policy.

8.2 Consent and withdrawal

The legal basis for loading the map is your consent (§ 25 Abs. 1 TDDDG, Art. 6(1)(a) GDPR). You give it by confirming that you are at least 16 years old and loading a map; on the iPhone, it applies to the map service you choose. If you are under 16, the law does not allow you to consent on your own; in that case, tap "Continue without map" and you will see the restaurants as a list with their addresses. The app only stores your decision on your device. You can withdraw your consent at any time with effect for the future: on Android devices by turning off the "Map display" switch in the app's settings, on the iPhone by choosing "No map" under "Map display" there. After that, the app no longer loads a map. On the iPhone, you can also switch the map service under "Map display"; the app then no longer loads the map of the previous service.

8.3 Your location

The app does not ask for your location itself. If you have allowed the app to access your location in your device settings, the loaded map shows your position as a dot; on iPhones, this may also lead your device to ask you for permission the first time the map loads. Your position is processed by the map service whose map you have loaded (section 8.1); we do not receive or store your position. You can withdraw location access at any time in your device settings. With "Directions" on a restaurant's page, you open its location outside the app in a map service, on the iPhone in Apple Maps or Google Maps as you choose; the privacy terms of its provider apply there. The order portal does not access your location; there, "Get directions" opens Google Maps in a new tab, and Google's privacy terms apply.

9. Usage analytics

The app does not currently use any usage analytics. If we introduce it, we will ask for your consent in the app beforehand and add to this section.

10. Contact form ("Feedback")

10.1 Which data

Using "Feedback", you can send us a message with a category, a subject and up to five pictures from your photo library, for example a question, a complaint or an enquiry about press, partnerships or franchising. We process your message, the pictures and your customer account data to deal with your request; we deal with requests about a booking together with the operating company (section 2.3). If your message otherwise concerns a particular restaurant, we pass it on, where necessary, with your name and contact details to that restaurant's operating company; the operating company then deals with your request under its own responsibility. We store messages and pictures with our service provider Supabase. Please do not upload pictures of other people without their permission.

The "Feedback" contact form is only available in the app. If you use the order portal, you can reach us by e-mail at media@citychicken-nhas.de or through the contact form on our website, which is covered by the website's privacy policy.

10.2 Legal basis

If your request concerns your customer account or a booking, the legal basis is Art. 6(1)(b) GDPR. Otherwise, we base the processing and the passing on to the operating company on Art. 6(1)(f) GDPR; our legitimate interest is to answer your enquiry. We only process information about health problems, for example after a visit to a restaurant, to clarify your complaint and to examine possible claims (Art. 9(2)(f) GDPR), and we only pass it on to the operating company of the restaurant concerned.

11. Security and protection against misuse

11.1 Requests to our interface

Our interface runs on Cloudflare; for technical reasons, every request from the app transmits your IP address. Requests from the order portal are first received by our server at Vercel (section 11.5), which forwards them to the interface together with your IP address so that the following limits apply to each guest individually; so that nobody can fake another person's IP address, our server marks it in a way that cannot be forged. To fend off misuse and attacks, we count requests to the interface:

- per IP address,
- per e-mail address for sign-in attempts,
- per customer account after sign-in.

These counters expire after about one hour at most. The checksums under which we count also remain in the logs of our interface for up to 7 days (section 11.9). Our server at Vercel also counts how often codes are requested and checked, sign-ins are set up and videos are converted from an IP address, and how often a customer account changes its profile picture, requests cancellations or refunds, exports its data or requests its deletion. Each of these counters applies for one to ten minutes; for this purpose, our server only keeps your IP address in its working memory, and for no more than ten minutes.

11.2 Sign-in and sessions at Supabase

When you register, sign in with codes or confirm your mobile number, and each time the app renews your sign-in, the app connects to Supabase or we pass your IP address on to Supabase. Supabase processes your IP address to detect and limit abusive sign-in attempts. So that you stay signed in, Supabase also stores each session with the IP address until you sign out, the session expires or your customer account is deleted (Art. 6(1)(b) and (f) GDPR). Supabase deletes logs of these events after 7 days. In the order portal, your browser connects to Supabase directly in part (section 3.2); signing in with a code sent by text message and every renewal of your sign-in go through our server at Vercel, which passes your IP address on to Supabase in the process.

11.3 Security logs

We log security-related events such as sign-ins, agreements to the Terms and Conditions, payments, cancellations, refunds and changes to the customer account with a shortened IP address and the identifier of the app and operating system (user agent), and for sign-in attempts with an e-mail address for which there is no customer account yet also with this address; this also happens in the first step of every registration. For events in the order portal, the log also contains your shortened IP address, but no identifier of your browser. We keep entries that prove the conclusion or performance of a contract for as long as the related bookings or your customer account; we delete all other entries after one year, unless we need individual entries for longer to investigate a specific security incident.

11.4 Legal basis

The legal basis is our legitimate interest in operating the app and the order portal securely and in protection against misuse and fraud (Art. 6(1)(f) GDPR). Cloudflare also processes certain information derived from the data traffic under its own responsibility, for example to detect attacks.

11.5 Server of the order portal at Vercel

We run the order portal on servers of Vercel Inc., 440 N Barranca Ave #4133, Covina, CA 91723, USA, as our processor. Vercel receives your requests in the data centre of its worldwide network that is closest to you and decrypts them there; if you use the order portal in Germany, this is usually a data centre in the European Union. The server functions of the order portal run in Frankfurt am Main; Vercel may carry out preliminary checks when a page is requested, such as renewing your sign-in, in the data centre that receives the request. With every request, our server checks your sign-in using the cookie bp-auth-token, renews it with Supabase where necessary and forwards your requests to our interface; in doing so, it passes your IP address on to the interface and to Supabase (sections 11.1 and 11.2). It does not store the content of your requests permanently; it keeps your initials and the reference to your profile picture for the header of our website in its working memory for about one minute. It delivers pictures of the menu in a suitable size; your browser loads videos directly from Supabase or, if it cannot play the video format, as a converted file from our server. Vercel records technical log data for every request, such as the IP address, the time, the address requested and information about your browser, and deletes it after 30 days at the latest. The legal basis is Art. 6(1)(b) GDPR insofar as our server handles requests about your customer account and your bookings, and otherwise our legitimate interest in a secure and fast order portal (Art. 6(1)(f) GDPR). Section 15.1 explains the transfer to the USA.

11.6 How we protect your data

We only transmit your data in encrypted form between the app or your browser and our servers. At our company and at the operating company, only people who need your data for their tasks can access it. Our processors are contractually obliged to process your data only on our instructions and to protect it with appropriate technical and organisational measures (Art. 28 and 32 GDPR).

11.7 Check before a code (Cloudflare Turnstile)

Before we send you a code by e-mail or text message, that is when you register, when you sign in, when you confirm your mobile number and when you request a code again, we use the Turnstile service of Cloudflare, Inc. to check whether the request comes from a human. This prevents programs (bots) from requesting codes in large numbers, for example to run up costs with text messages to other people’s numbers or to create customer accounts in bulk. From version 1.1.0, the app opens a page of our interface (api.nhascitychicken.app) in the background for this, which loads the check from Cloudflare (challenges.cloudflare.com) as soon as you open registration or sign-in or confirm your mobile number; so that you do not have to wait, it already prepares the check for the next code after each code. In the order portal, your browser loads the check from Cloudflare only on the page for sign-in and registration, as soon as you open it, even before you enter anything there, and there too it prepares the check for the next code after each code. If Cloudflare is unsure, we ask you to confirm with a tick that you are not a bot; otherwise the check runs without any action on your part.

For the check, Cloudflare’s program carries out small computing tasks on your device and reads characteristics of your device and of the view in which the check runs, such as which functions it supports and how the check is operated. It sends this information to Cloudflare together with your IP address, characteristics of your encrypted connection, the identifier of the app or of your browser (user agent) and the address of the page. In the order portal, Cloudflare’s program runs in our page and also passes on to Cloudflare’s check frame the full address of the page with all the information it contains, for example the page you return to after signing in, together with information on the structure of the page and on our

scripts, the size of your window and the address you came from. In addition, Cloudflare's program asks servers of Cloudflare and of Google via WebRTC for the public address of your internet connection; Google also receives your IP address in the process. Cloudflare may store cookies, entries in local storage and small files that record the status of the check, make it possible to follow how the check is operated and help Cloudflare detect faults; in the app, they only remain until the app closes the view for the check, for example when you leave the sign-in. On Android, the app then deletes them itself and, if it was shut down before, the next time it starts. In the order portal, when the page for sign-in and registration is first loaded, Cloudflare creates, without any action on your part, an entry with a random string of characters and a small file, which remain in your browser without an expiry date; Cloudflare's program reads the entry at every check, including the first, and transmits it to Cloudflare, so that Cloudflare can recognise your browser in later checks on our website. It is not necessary for the sign-in you open that both of them remain after the check, and we cannot delete them (section 12.4). Cloudflare assesses the information and returns proof of the check to the app or to your browser, which our server has Cloudflare confirm, together with your IP address; in the order portal, our server at Vercel passes the proof on to our interface for this. We do not pass your name, your e-mail address or your mobile number on to the check.

If the request has passed the check or we cannot reach Cloudflare at that moment, our server creates an approval for exactly one code in our database. For this, we only store a checksum of your e-mail address or of the identifier of your customer account and the time at which the approval expires, not the address itself; because we form this checksum without a secret key, it can be matched to a known address. The approval is valid for five minutes. We delete it as soon as the code has been sent, and otherwise at the hourly clean-up after it has expired. If the check fails, the app, or in the order portal your browser via our server at Vercel, reports Cloudflare's error code or the reason why no check took place, together with the platform and the version of the app or of the order portal, to our interface so that we can identify faults on particular devices; this report is only kept in the logs of our interface (section 11.9).

For the check, Cloudflare processes the information as our processor. According to Cloudflare, it also uses the same information under its own responsibility to improve Turnstile's bot detection for all websites and apps that use Turnstile, and bases this on its legitimate interest; you can find more about this in the Turnstile Privacy Addendum and in Cloudflare's privacy policy. We are responsible for embedding the check and for transmitting the information to Cloudflare and to Google; Cloudflare, Inc. is responsible for using it to improve Turnstile, and Google LLC for processing the requests that Google receives; you can find more about this in Google's privacy policy. Section 15.1 applies to the transfer to the USA and to other countries.

The legal basis for storing and reading information on your device is § 25 Abs. 2 Nr. 2 TDDDG, because this is strictly necessary so that we can provide you with the registration and sign-in that you open in a form that is protected against misuse. This does not apply to the entry and the file that Cloudflare leaves in your browser in the order portal beyond the check (section 12.4). We base the other processing for the check on our legitimate interest in sending codes only to humans, in preventing costs caused by text messages requested for misuse and by customer accounts created in bulk, and in protecting our systems (Art. 6(1)(f) GDPR). We base the fact that Cloudflare also receives the information to improve Turnstile on our legitimate interest and on Cloudflare's legitimate interest in effective bot detection, on which the protection of your customer account also depends (Art. 6(1)(f) GDPR). We base the fact that Google receives your IP address during the check on our legitimate interest in the check, for which Cloudflare's program makes these requests (Art. 6(1)(f) GDPR). If a request does not pass the check, we may not send a code. If the check permanently fails on your device, write to us at media@citychicken-nhas.de.

11.8 Sending text messages and limits for codes

A function at Supabase in Ireland passes each text message with a code to Twilio, which sends it. For this, Supabase passes the function the details of your customer account, including your mobile number, the code and the IP address from which the request comes. Before the function passes the text message to Twilio, it checks whether the number is a mobile number from a member state of the European Union or from Switzerland, whether there is an approval under section 11.7 and whether one of our limits has been reached: per mobile number, per customer account and, for new numbers, per network, we only send a limited number of text messages per hour and per day. If the number is not such a mobile number or a limit has been reached, we do not send the text message and tell you why in the app or in the order portal; the same applies without an approval once we make the check under section 11.7 mandatory.

So that we can apply the limits, we only store, for each text message sent, the time, the identifier of your customer account, a checksum of your mobile number formed with a secret key, whether it is a new number and, for a new number, a checksum of your network formed in the same way, that is of your IPv4 address or of the address range of your IPv6 address. We do not store your number or your IP address there in plain text, and we store nothing there for refused requests. We delete these entries every hour as soon as they are older than 25 hours. The logs of the function show, for each request, the result, the reason for any refusal, the country, whether it is a new number and your number only with the country code and at most the last four digits (section 11.9).

The legal basis for sending the text message is Art. 6(1)(b) GDPR (section 3.3). We base the checks, the counting and the logs on our legitimate interest in sending codes securely and in preventing misuse and costs caused by text messages requested in large numbers (Art. 6(1)(f) GDPR).

11.9 Logs of our interface and our functions

Our interface at Cloudflare and our functions at Supabase that send e-mails and text messages with codes write logs so that we can detect and fix errors and attacks. The logs and traces of the interface contain, for each request, the time, the type of request, the address called, which may contain an order number, for example, the result and the duration, your full IP address and the location that Cloudflare derives from it (country, region, city, postcode, approximate coordinates and time zone), your network operator, the Cloudflare data centre, features of your encrypted connection, the identifier of the app or your browser with the operating system (user agent), your language setting and other headers of the request; Cloudflare masks your sign-in token. The traces also record which services the interface calls in the process, such as Supabase, Stripe or the point-of-sale system, with the address called, the result and the duration; these addresses may contain identifiers such as Stripe's payment reference. They also contain messages from our programs, such as whether the check under section 11.7 was passed, but not the proof itself, an error code together with the platform, the version of the app or of the order portal and the step in which the check failed, or, when you sign in, the number of your customer account, and the identifiers under which we count requests under section 11.1; these are checksums of your IP address, your e-mail address or the identifier or the number of your customer account, formed with a secret key. The logs of the functions contain, for each request, the result and the reason for any refusal, for e-mails only the domain of the address, such as gmail.com, and for text messages the details under section 11.8. Cloudflare and Supabase delete these logs after 7 days at the latest. The legal basis is our legitimate interest in the secure and stable operation of the app and the order portal (Art. 6(1)(f) GDPR).

12. Data on your device and in your browser

12.1 What the app stores

The app only stores on your device what it needs in order to work:

- your sign-in or, if you continue without an account, only that choice, and the language you have chosen,
- your basket during an order,
- a copy of your QR ticket so that you can show it even without an internet connection, at the most until you have checked in or the booking is cancelled; if the app is not open then, it deletes the copy the next time you open it,
- cached pictures and videos, for example of the menu and the restaurants,
- your decision about the restaurant map (section 8),
- map data cached by the map service you chose (section 8),
- the installation ID and token for push notifications (section 7),
- the identifiers of Stripe's payment module (section 6.2),
- your till receipt as a PDF file in the app's cache as soon as you view it (section 5.8),
- the version of the Terms and Conditions and of this Privacy Policy that was last loaded, so that you can read them without an internet connection,
- from version 1.1.0, the entries and files that Cloudflare stores in the view for the check before a code, until the app closes the view or, if it was shut down before, until it next starts (section 11.7).

A file with your data that you export (section 16.2) remains on your device until you delete it.

12.2 Deletion in the app

When you sign out, the app deletes your sign-in, the copy of your QR ticket, cached till receipts, the stored copy of the push token and your decision about the restaurant map; it also deletes the copy of the QR ticket when you have checked in or the booking is cancelled. You can remove everything else by deleting the app.

12.3 Legal basis for the app

The legal basis for storing this information is § 25 Abs. 2 Nr. 2 TDDDG, because this is necessary for the functions you use; section 8 applies to the map, and section 11.7 to the check before a code. The app does not read your device's advertising identifiers, and it does not set any cookies for advertising or analytics purposes.

12.4 What the order portal stores in your browser

The order portal only stores in your browser what is needed for the functions you use there; what Cloudflare stores beyond that during the check before a code is set out at the end of this section. Other websites cannot read the entries on our domain. Your browser only sends the order portal's cookies over encrypted connections.

Entry	Purpose	Content	Lifetime	Legal basis
bp-auth-token, split into bp-auth-token.0 and bp-auth-token.1 for larger sign-ins (cookie)	Keeps you signed in to the order portal.	The keys of your sign-in and details from your customer account such as its identifier, your e-mail address and your mobile number. Your browser only sends it to addresses under citychickennhas.de/bestellen; scripts on our pages cannot read it.	If you do not tick the box to stay signed in, a session cookie; it ends when you close your browser, unless your browser restores your last session. If	§ 25 Abs. 2 Nr. 2 TDDDG; Art. 6(1) (b) GDPR

Entry	Purpose	Content	Lifetime	Legal basis
			you tick it, 30 days after you last used the order portal; every use and every renewal of your sign-in extends this period. It always ends when you sign out.	
bp_remember (cookie)	Remembers that you have chosen to stay signed in.	Only the value “1”. We only set it if you tick the box. Your browser only sends it to addresses under citychickennhas.de/bestellen; scripts on our pages cannot read it.	As long as your sign-in with the box ticked, that is, 30 days after you last used the order portal. It ends when you sign out or your sign-in expires.	§ 25 Abs. 2 Nr. 2 TDDDG
bp_present (cookie)	Tells the header of our website that someone is signed in to the order portal in this browser (section 13.2).	Only the value “1”. We only set it after you have signed in.	Same as bp-auth-token.	§ 25 Abs. 2 Nr. 2 TDDDG
bp_pay_pending (cookie)	Ensures that we only accept a return from Klarna for exactly this order.	Your order number and the identifier of your payment at Stripe. We set it when you click “Order and pay” or “Pay now”.	30 minutes.	§ 25 Abs. 2 Nr. 2 TDDDG; Art. 6(1) (b) GDPR
bp_pay_return (cookie)	Shows the result of the payment on the page of your order after you return from Klarna.	Your order number and the result of the payment.	Two minutes.	§ 25 Abs. 2 Nr. 2 TDDDG; Art. 6(1) (b) GDPR
bp-cart:v1 (local storage)	Keeps your basket when you reload the page or open another tab.	The food and drinks with your choices and quantities, the restaurant and a random identifier, but not your customer number. We only create the entry when you put the first item in your basket or when we put the food and drinks of a cancelled order that was not paid for back into your basket.	Until you order, until you sign out or until you sign in again, for no more than seven days; the order portal discards older entries.	§ 25 Abs. 2 Nr. 2 TDDDG; Art. 6(1) (b) GDPR
bp-clips (local storage)	Remembers whether you have paused the menu videos.	“on” or “off”. We only create the entry when you pause or play the videos.	Until you delete the site data in your browser.	§ 25 Abs. 2 Nr. 2 TDDDG
NEXT_LOCALE (cookie)	Our website sets it if you choose a language other	The code of the language you have chosen.	Until you close your browser, unless your	§ 25 Abs. 2 Nr. 2 TDDDG

Entry	Purpose	Content	Lifetime	Legal basis
	than the one your browser indicates; the order portal then opens in this language.		browser restores your last session.	
__stripe_mid (Stripe cookie)	Fraud prevention for the payment (section 6.5).	A random identifier of your browser at Stripe. Stripe.js only sets it on the checkout page; it applies to our entire domain.	One year; the lifetime starts again as soon as Stripe.js is loaded again.	§ 25 Abs. 2 Nr. 2 TDDDG; Art. 6(1) (f) GDPR
__stripe_sid (Stripe cookie)	Fraud prevention for the payment (section 6.5).	A random identifier of your session at Stripe. Stripe.js only sets it on the checkout page; it applies to our entire domain.	30 minutes; the lifetime starts again as soon as Stripe.js is loaded again.	§ 25 Abs. 2 Nr. 2 TDDDG; Art. 6(1) (f) GDPR
m (Stripe cookie for the domain m.stripe.com)	Fraud prevention for the payment (section 6.5).	An identifier of your browser at Stripe, set, according to Stripe, when Stripe.js loads on the checkout page.	According to Stripe, up to two years.	§ 25 Abs. 2 Nr. 2 TDDDG; Art. 6(1) (f) GDPR

During the check before a code, Cloudflare also creates two entries on the page for sign-in and registration in the storage that your browser allocates to Cloudflare's page (challenges.cloudflare.com): in local storage the entry cf.turnstile.u with a string of 149 random-looking characters, and in your browser's file storage (Origin Private File System) a file with a single byte under a fixed name that is the same in every browser. Both are created, without any action on your part, when the page is first loaded and remain without an expiry date; Cloudflare's program reads the entry at every check and transmits it to Cloudflare, and it writes the file again at every check. It is not necessary for the sign-in you open that both of them remain after the check, and we cannot delete them; you can delete them in your browser's settings. Whether Cloudflare can also read them on other websites that use Turnstile depends on whether your browser separates this storage by website; Chrome and Firefox on computers do so in their default settings (section 11.7).

In addition, your browser keeps pictures and videos of the menu for up to one year and your profile picture for no more than five minutes in its cache so that the pages load faster. If you export your data in the order portal (section 16.2), the downloaded file remains on your device until you delete it. You can find an overview of all cookies and entries on citychickennhas.de in our website's privacy policy.

12.5 Deletion and legal basis in the order portal

When you sign out in the order portal or through the account icon on our website, we delete the cookies bp-auth-token, bp_remember and bp_present and your basket. We also delete your basket as soon as you order and when you sign in again. If you delete your customer account in the order portal, we sign you out on all devices and also delete these entries in your browser. The other entries expire as stated in section 12.4; you can delete them at any time in your browser settings.

The legal basis for storing and reading this information is § 25 Abs. 2 Nr. 2 TDDDG, because this is necessary for the functions you use: signing in, and if you tick the box to stay signed in also beyond closing your browser, showing that you are signed in in the header of our website, the basket, payment, the

language setting and your setting for the videos; section 6.5 applies to Stripe and section 11.7 to the check by Cloudflare. We process the data in these entries on the basis of Art. 6(1)(b) GDPR insofar as it is necessary for your customer account and your order, and otherwise on the basis of our legitimate interest in a secure and easy-to-use order portal (Art. 6(1)(f) GDPR). The order portal does not set any advertising or analytics cookies.

12.6 Connection check in older app versions

Versions of the app up to and including 1.0.0 call a test address operated by Google (clients3.google.com) on iPhones when the app starts, whenever the network changes and, while the app is open, about once a minute, or every five seconds if there is no answer; this also applies while the app only asks you to update. Google receives your IP address and the technical details of the request, such as the identifier of the app and the operating system. This check is a default setting of a software library; the app does not use its result, because it learns from your operating system whether you are offline. We can no longer switch the check off in a version that is already installed; from version 1.0.1, it no longer takes place. Please update the app for this reason. The check does not take place on Android devices. Until you update, the legal basis is our legitimate interest in continuing to provide the version of the app that you have installed (Art. 6(1)(f) GDPR).

13. Our websites

13.1 Legal texts on our website and addresses at nhascitychicken.app

We publish this Privacy Policy, our Terms and Conditions and our accessibility information on our website at citychickennhas.de/en/datenschutz/kundenkonto, citychickennhas.de/en/agb and citychickennhas.de/en/barrierefreiheit; you can also read the Terms and Conditions and the Privacy Policy directly in the app. The website's privacy policy applies to visits to these pages; we do not load any services for audience measurement or advertising on them. If you open an earlier address of these texts at nhascitychicken.app, we show you the same version there or permanently redirect you to our website; we provide the PDF files of our legal texts at nhascitychicken.app. Cloudflare delivers the pages, redirects and files at nhascitychicken.app for us; pictures on these pages come from our service provider Supabase. For technical reasons, your IP address, the date and time of access, the address requested and information about your browser are processed in order to deliver them and protect them against attacks. These pages and redirects are delivered by the same interface that the app uses; requests for them therefore remain in its logs for no more than 7 days with the details listed in section 11.9, including the location that Cloudflare derives from your IP address. The legal basis is our legitimate interest in secure delivery (Art. 6(1)(f) GDPR). We do not use cookies or tracking for this. Sections 11.5 and 12.4 explain how the pages of the order portal are delivered and what your browser stores there. Cookies on citychickennhas.de are covered by the website's privacy policy.

13.2 Account icon in the header of our website

If you are signed in to the order portal, the header of our website citychickennhas.de shows an account icon with your profile picture or your initials. When you open it, it takes you to your orders, your profile and signing out. For this, the website checks whether the cookie bp_present is set in your browser and only then requests your initials and your profile picture from our server; your browser sends the cookie bp-auth-token with this request, and this may extend your sign-in (section 12.4). Your initials are not part of the text of the page. We only show this information to you; we do not pass it on to the analytics and advertising services that run on the website only with your consent. If you go from the order portal to the other pages of the website, these services only learn that you came from our domain, not from which page of the order portal. The legal basis is § 25 Abs. 2 Nr. 2 TDDDG for reading the cookies and Art. 6(1)(b)

GDPR for showing your details as part of your customer account. All other processing on the website is covered by the website's privacy policy.

14. Recipients and service providers

14.1 Who receives data

Your data is only received by those who need it for the purposes described: the staff and the administration of the operating company of the booked restaurant (section 5), the operating company of a restaurant if your request concerns that restaurant (section 10), the operating company's bank for a refund by bank transfer (section 6.1), and these service providers:

Recipient	**Task**	**Role**	**Registered office and place of processing**
Supabase Pte. Ltd., Singapore	Database, customer accounts and sign-in, in the order portal also directly from your browser (section 3.2), file storage, creation of the e-mails with codes, passing the text messages with codes to Twilio and limits for text-message codes (section 11.8), delivery of the menu videos in the order portal	Processor	Singapore; processing in Ireland (EU) (section 15.2)
Cloudflare, Inc., San Francisco, USA	Interface with its logs (section 11.9), pages, redirects and PDF files at nhascitychicken.app, protection against misuse and the check before a code (Turnstile, section 11.7), connection to the database, fallback for sending the booking confirmations and other e-mails about bookings (Cloudflare Email Service), forwarding of e-mails to our sender address accounts@nhascitychicken.app, receiving the till receipts by e-mail and storing them briefly in a storage facility in the EU (section 5.8)	Processor; under its own responsibility for derived network data and for improving Turnstile	USA; worldwide network of data centres (section 15.1)
Plus Five Five, Inc. (Resend), San Francisco, USA	Sending the e-mails with codes, the booking confirmations and other e-mails about bookings (sections 3.2 and 5.3)	Processor, for e-mails about bookings also for the operating company	USA; sending from Ireland (EU), storage of the e-mails in the USA (section 15.1)
Twilio Ireland Limited, Dublin, Ireland, with Twilio Inc., San Francisco, USA	Sending the codes by text message	Processor; under its own responsibility for usage and security data	Ireland and USA; processing in the USA
Google LLC, Mountain View, USA	Push notifications in the app (Firebase Cloud Messaging)	Processor	USA; worldwide processing
Google LLC, Mountain View, USA	Checking the internet connection in older app versions on iPhones (section 12.6)	Under its own responsibility	USA; worldwide processing
Google LLC, Mountain View, USA	Answering the requests of Cloudflare's program during the check before a code (section 11.7)	Under its own responsibility	USA; worldwide processing

Recipient	Task	Role	Registered office and place of processing
Apple Distribution International Limited, Cork, Ireland	Delivery of push notifications to iPhones (Apple Push Notification Service); restaurant map on the iPhone (Apple Maps), only after your consent; Apple Pay if you choose it in the app or in your browser	Under its own responsibility as the provider of the operating system and of Apple Pay (section 6.4) and for the further use of the map data (section 8.1)	Ireland; according to Apple, transfer to the USA on the basis of standard contractual clauses
Google Ireland Limited, Dublin, Ireland	Restaurant map in the app (Google Maps), only after your consent; Google Pay if you choose it in the app or in your browser	Under its own responsibility for further use (sections 6.4 and 8.1)	Ireland; transfer to Google LLC in the USA possible
Stripe Payments Europe, Limited, Dublin, Ireland, with other Stripe companies	Payment processing for the operating company; payment field and fraud prevention on the checkout page of the order portal (section 6.5); Link if you use it in the app	Processor for the operating company; otherwise under its own responsibility (sections 6.2 to 6.5)	Ireland; transfer to Stripe, LLC in the USA
Lightspeed Netherlands B.V., Amsterdam, Netherlands, with Lightspeed Commerce Inc., Montréal, Canada	The restaurant's point-of-sale system (Lightspeed Restaurant): receiving your order at check-in, screen and ticket for the kitchen, recording in the till and till receipt, sending the till receipt to us by e-mail through the SendGrid service in the USA (sections 5.7, 5.8 and 15.3)	Processor for the operating company	Netherlands and Canada; processing in data centres of Amazon Web Services and Google, also possible outside the EU (section 15.3)
Klarna Bank AB (publ), Stockholm, Sweden	Payment with Klarna if you choose Klarna	Under its own responsibility (section 6.4)	Sweden (EU)
Vercel Inc., Covina, USA	Hosting of our internal management system and of the order portal, including processing of profile pictures (section 11.5)	Processor, also for the operating company; under its own responsibility for its own usage and log data	USA; server functions in Frankfurt am Main (EU), requests received in the nearest data centre (section 15.1)
IONOS SE, Montabaur, Germany, with Microsoft Ireland Operations Limited, Dublin, Ireland, as sub-processor (Microsoft 365)	Mailboxes for e-mails to media@citychicken-nhas.de, to kontakt@citychicken-nhas.de, also for replies to the e-mails about your bookings, to the data protection officer and for internal notes about bookings	Processor, for e-mails about bookings also for the operating company	Germany and Ireland; storage in the EU

Recipient	Task	Role	Registered office and place of processing
IONOS SE, Montabaur, Germany	Mailbox mog@citychicken1993.de, also for withdrawals by e-mail	Processor for the operating company	Germany

14.2 Contracts and authorities

Processors are bound by contract to the instructions of the company responsible in each case. For joint processing, we also conclude these contracts in the name of the operating company; it concludes the contracts with Stripe and Lightspeed itself. Recipients acting under their own responsibility process and transfer data in accordance with their own privacy terms. Authorities, courts and advisers, such as the operating company's tax advisers, only receive data if we or the operating company are legally obliged to provide it or if this is necessary to assert or defend claims.

The operating company and our processors have contractually undertaken to protect your data as required by the GDPR and this Privacy Policy. Recipients acting under their own responsibility are themselves bound by the GDPR when processing your data or, where they are based in the United States, by the principles of the EU-U.S. Data Privacy Framework (section 15.1).

14.3 App stores

If you download the app from the App Store or Google Play, Apple (Apple Distribution International Limited, Ireland) and Google (Google Ireland Limited, Ireland) process the data needed for this, for example about your store account, under their own responsibility; we have no influence on this.

15. Transfers to third countries

15.1 United States and worldwide data centres

Some service providers process personal data outside the European Union and the European Economic Area, in particular in the United States of America, in Canada and in Singapore; Cloudflare, Google and Vercel also process data in their data centres around the world. For the United States, the European Commission found in Commission Implementing Decision (EU) 2023/1795 that organisations certified under the EU-U.S. Data Privacy Framework ensure an adequate level of protection (Art. 45 GDPR). We base transfers to Cloudflare, Inc., Twilio Inc., Google LLC, Vercel Inc. and Plus Five Five, Inc. (Resend) on this, and the operating company bases transfers to Stripe, LLC on it, as long as these companies are listed as actively certified in the official list at dataprivacyframework.gov.

Vercel receives requests to the order portal in its worldwide network of data centres, and Vercel Inc. can access data from the USA for operation and support; in addition to its certification under the EU-U.S. Data Privacy Framework, the standard contractual clauses in our data processing agreement with Vercel apply (Art. 45 and Art. 46(2)(c) GDPR).

Resend sends our e-mails from a data centre in Ireland, stores them with their content and the sending details, such as recipient, time and delivery status, in the USA and, according to Resend, deletes them after 30 days. In addition to the certification under the EU-U.S. Data Privacy Framework, the standard contractual clauses in our data processing agreement with Resend apply (Art. 45 and Art. 46(2)(c) GDPR).

Cloudflare operates a worldwide network of data centres. Requests from the app and from our server at Vercel to our interface and requests for addresses at nhascitychicken.app are handled by the data centre that receives the request; if you are in Germany, this is usually a data centre in the European Union. Cloudflare stores the counters for protection against misuse centrally and also keeps them in other data

centres for a short time. Cloudflare stores the logs and traces under section 11.9 in its core data centres, which may also be located outside the European Union. We have not restricted processing at Cloudflare to the European Union, including for sending and receiving e-mails and for the check before a code (section 11.7); your data may therefore also be processed outside the European Union, including in countries without an adequacy decision. This is based on the certification of Cloudflare, Inc. under the EU-U.S. Data Privacy Framework and on the standard contractual clauses in our data processing agreement with Cloudflare (Art. 45 and Art. 46(2)(c) GDPR). You can obtain a copy of the standard contractual clauses in our agreements with Vercel, Resend and Cloudflare on request at media@citychicken-nhas.de.

15.2 Singapore and standard contractual clauses

Our database, the customer accounts and the stored files are hosted by Supabase in an Amazon Web Services data centre in Ireland (EU); the functions that create our e-mails with codes and pass our text messages with codes to Twilio also run in Ireland. Supabase Pte. Ltd. is based in Singapore, for which there is no adequacy decision, and can access the data for operation and maintenance. The European Commission's standard contractual clauses (Commission Implementing Decision (EU) 2021/914) in our data processing agreement with Supabase apply to this (Art. 46(2)(c) GDPR). You can obtain a copy of the standard contractual clauses on request at media@citychicken-nhas.de.

15.3 The restaurant's point-of-sale system: Canada and other countries

The operating company's point-of-sale system is provided by Lightspeed Netherlands B.V. in Amsterdam. Its parent company, Lightspeed Commerce Inc. in Montréal (Canada), processes the data as a further processor. For Canada, the European Commission has found that organisations subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) ensure an adequate level of protection (Decision 2002/2/EC, which remains in force under Art. 45(9) GDPR). Where this decision does not apply, the European Commission's standard contractual clauses (Commission Implementing Decision (EU) 2021/914) in the operating company's data processing agreement with Lightspeed apply (Art. 46(2)(c) GDPR). Lightspeed runs the point-of-sale system in data centres of Amazon Web Services and Google, sends the till receipts through the e-mail service provider SendGrid in the USA and may use other group companies and service providers outside the European Union, including in the USA and in countries without an adequacy decision; processing is not contractually limited to the European Union. Lightspeed must safeguard such onward transfers with standard contractual clauses or, for recipients in the USA that are certified under the EU-U.S. Data Privacy Framework, rely on that framework (section 15.1). You can obtain a copy of the standard contractual clauses in the operating company's contract with Lightspeed on request at media@citychicken-nhas.de.

16. Storage period and deletion

16.1 Retention periods

We delete your data after these periods:

- **Customer account:** when you delete it, in the app under Profile → Settings → "Delete Account", in the order portal under "Profile", or by sending an e-mail to media@citychicken-nhas.de. Once you have asked for it to be deleted, your customer account is deactivated immediately, and we sign you out on all devices. If you sign in again with a code in the app or in the order portal within 30 days, it is restored; simply opening a page does not restore it. After 30 days, we delete your name, e-mail address, mobile number, country, profile details including pictures, push tokens, your list of notifications, ratings on bookings, your till receipts with the related details, your sign-in data at Supabase and your messages and pictures from the contact form. What was passed to the restaurant's point-of-sale system at check-in remains stored there as described in section 5.7, including your first

name. What remains is a record with your customer number, without your name or contact details, which keeps your bookings together; we delete it together with the bookings. If a refund for a takeaway order is still open, the point “Bookings and payments” applies to it.

- **Bookings and payments (section 5.1):** ten years from the end of the calendar year in which you booked, and longer only as long as they are relevant to a tax assessment that is still open. The operating company must keep books and records for this long, and accounting vouchers, including invoices, for eight years (Art. 6(1)(c) GDPR in conjunction with § 147 AO (German Fiscal Code), § 257 HGB (German Commercial Code) and § 14b UStG (German Value Added Tax Act)). If you delete your customer account, this data remains stored without your name and contact details. If, for a takeaway order, the refund for sealed drinks or sauces is still open because the return is pending or the refund is still under way or has failed, we keep your name and e-mail address with that order until the refund has been settled or the restaurant has closed the case without a refund, at most until the end of the third calendar year after the year in which it fell due, so that we can reach you about it (section 6.1). You can cancel an order that you do not pay for; otherwise our system cancels it once the period for paying has expired. It is kept like a booking.
- **Refund made another way (section 6.1):** The operating company keeps the record of a bank transfer with your name and bank details and the receipt for a cash payment for eight years from the end of the calendar year in which they were created (Art. 6(1)(c) GDPR in conjunction with § 147 AO and § 257 HGB); we keep our e-mail about it and your reply with your bank details like other e-mails about the performance or unwinding of a contract.
- **The restaurant’s point-of-sale system (section 5.7):** ten years from the end of the calendar year in which your order was recorded in the till, and longer only as long as the records are relevant to a tax assessment that is still open; after that, the operating company has them deleted (Art. 6(1)(c) GDPR in conjunction with § 147 AO and § 257 HGB).
- **E-mails with till receipts (section 5.8):** as soon as we have matched the till receipt to your booking; if it cannot be matched to a booking, seven days after it arrived; till receipts for a refund made at the till immediately. In any case, the storage facility at Cloudflare deletes every e-mail after 30 days at the latest.
- **Holds:** seven days after they end.
- **Abandoned registration:** If you abandon registration in the app or in the order portal before you have saved your personal details, we delete your sign-in data at Supabase seven days after you started registering. If you have already saved them, your customer account already exists, and the period for the customer account applies.
- **Records relating to the Terms and Conditions and the Privacy Policy:** we store the details listed in section 3.1 about your agreement, our notice or your acknowledgement as long as your customer account exists, and after that, without your name and contact details, until the end of the third calendar year after your customer account is deleted. The version of the Terms and Conditions that applies to a booking is stored with the booking (section 5.1).
- **Push notifications:** delivery logs with your device token after 90 days, read notifications in your list of notifications one year after you read them, and otherwise together with your customer account.
- **Contact form:** together with your customer account (see above); if you wish, we delete individual messages and pictures earlier.
- **Check before a code (section 11.7):** approvals as soon as the code has been sent, otherwise at the hourly clean-up after they have expired; an approval is valid for five minutes. Cloudflare decides how

long it keeps the information from the check; in its information on Turnstile, Cloudflare does not state a period for this. Google decides how long it keeps the requests made during the check.

- **Sending of text messages (section 11.8):** entries on text messages sent, every hour as soon as they are older than 25 hours.
- **E-mails at Resend (sections 3.2, 5.3 and 15.1):** according to Resend, after 30 days.
- **E-mails to our mailboxes, including replies to our e-mails about your bookings (sections 2.4, 3.2 and 5.3):** If an e-mail concerns the conclusion, performance or unwinding of a contract, for example because you withdraw from, cancel or complain about a booking in it, request a refund or show that you have sent items back, we keep it together with its attachments for six years from the end of the calendar year in which it arrived, and longer only as long as it is relevant to a tax assessment that is still open (Art. 6(1)(c) GDPR in conjunction with § 257 HGB (German Commercial Code) and § 147 AO (German Fiscal Code)). For e-mails about a booking, we do this for the operating company, which alone is responsible for keeping them (section 2.5). The operating company keeps letters in which you withdraw from a contract, cancel a booking or ask for a refund in the same way. We delete all other e-mails and our internal notes about bookings once the matter has been dealt with, at the latest six months after the last message about it.
- **Security logs:** as stated in section 11.3; **records of access in our management system:** as stated in section 5.2; **counters for protection against misuse:** after about one hour at most, and at our server at Vercel after ten minutes at most (section 11.1); **sign-in logs at Supabase:** as stated in section 11.2; **logs at Vercel:** after 30 days at the latest (section 11.5); **logs of our interface at Cloudflare and of our functions at Supabase:** after 7 days at the latest (section 11.9).
- **Data on your device and in your browser:** as described in section 12.

16.2 Data export and access

As long as your customer account exists, you can export the data that we store about you in your customer account yourself: in the app under Profile → Settings → “Export My Data” as a file that you can download or display, and in the order portal under “Profile” as a file in JSON or CSV format. The file contains your customer account data and your bookings, including the identifier of your ticket, the payment reference and, after check-in, your pickup number, the copy of the receipt data and the number of your till receipt, but no security values such as check values of codes; you can save the till receipt itself as a PDF file with your booking (section 5.8). Once you have asked for your customer account to be deleted, the export is no longer possible. If you ask us at media@citychicken-nhas.de, we will also provide you with the same file. If you ask us at the same address, you will receive full information about all the data that we and the operating company process about you, including logs, data held by our service providers and data in the restaurant’s point-of-sale system, within one month.

17. Your rights

17.1 Your rights at a glance

You have the right to access your data, to have it corrected or erased, to have its processing restricted and to data portability (Art. 15 to 18 and 20 GDPR). You can withdraw consent at any time with effect for the future, for the restaurant map with the switch in the app (section 8.2). At present, you cannot change your e-mail address or your mobile number yourself, either in the app or in the order portal; to do so, write to us at media@citychicken-nhas.de or use the contact form on our website.

Right to object (Art. 21 GDPR): Where we process data on the basis of our legitimate interest (Art. 6(1)(f) GDPR), you have the right to object, on grounds relating to your particular situation, at any time to this

processing. We will then no longer process the data. An exception applies if we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms. An exception also applies if the processing is for the establishment, exercise or defence of legal claims.

17.2 How to exercise your rights

You can delete your customer account yourself in the app and in the order portal and export your data there, in the order portal even if you have not yet agreed to new Terms and Conditions (section 16). For all other requests, and also for deletion and export if you prefer to write to us, contact media@citychicken-nhas.de or our data protection officer (section 2.6). We are your central point of contact, including for booking data for which we are jointly responsible with the operating company.

17.3 Complaint to a supervisory authority

You can lodge a complaint with a data protection supervisory authority (Art. 77 GDPR), in particular in the Member State of your place of residence, your place of work or the place of the alleged infringement. The authority responsible for Nhas Food 1993 GmbH and MOG Gastro GmbH is the Berlin Commissioner for Data Protection and Freedom of Information (Berliner Beauftragte für Datenschutz und Informationsfreiheit), Alt-Moabit 59–61, 10555 Berlin, e-mail mailbox@datenschutz-berlin.de, www.datenschutz-berlin.de.

17.4 Automated steps and human review

We do not make any decisions based solely on automated processing which produce legal effects concerning you or similarly significantly affect you (Art. 22 GDPR). The only steps that run automatically are those that apply the agreed booking rules without assessing you personally, for example these: the app and the order portal check the number of people, the booking period, the minimum order value, maximum quantities and the maximum order value and only let you order once your order complies with these rules; they refuse a booking if the time slot is fully booked, you have reached the number of time slots that the restaurant allows per business day, or prices have changed. An expired hold is released and an unpaid order is cancelled. If you cancel, our system calculates the refund amount according to the booking rules: until the deadline for free cancellation the full price, after that the share you were given before you ordered. If your ticket expires without you having checked in or cancelled, our system cancels the booking and refunds the share according to the booking rules, and a booking that the restaurant has refunded in full is cancelled. Where changed Terms and Conditions require your agreement before you can book again, you cannot reserve or book any new time slots until you have agreed. Depending on its version, the app also locks its other functions until then, but from version 1.1.0 not your orders and “Withdraw from contract”; in the order portal you can still view and cancel your existing bookings, request the refund where clause 15.3 of the Terms and Conditions still provides for this, withdraw via “Withdraw from contract”, delete your customer account and export your data. You can also ask us by e-mail at any time to delete your customer account or export your data (section 17.2). Automated checks also run before a code: our system checks whether the e-mail address meets the requirements under section 3.2, before a text message whether the number is a mobile number from the European Union or Switzerland and whether a limit under section 11.8 has been reached, and, once we make the check under section 11.7 mandatory, whether it has been passed; depending on the result, we do not send the code. The check under section 11.7 only assesses, on the basis of the characteristics of your device and how the check is operated, whether the request comes from a program; if Cloudflare is unsure, you can clarify this with a tick. If you think such a step is wrong, write to us at media@citychicken-nhas.de. A person at the operating company or one of our staff will then review your case, and you can explain your point of view. Stripe carries out fraud checks on payments under its own responsibility (section 6.3).

18. Children and young people

18.1 Minimum age and parental consent

You may use the app and the order portal from the age of 13. If you are not yet 18, you need the consent of your parents or other persons with parental custody for your customer account and your bookings, as described in the Terms and Conditions. Until they have decided, we process your data because you have asked us to let you use the platform (Art. 6(1)(b) GDPR). If they refuse, we delete your customer account as soon as they or you tell us; the operating company only keeps booking data for as long as the law requires it to (section 16).

18.2 Consent under data protection law

We only ask for consent under data protection law for the restaurant map in the app (section 8). If you are under 16, you cannot give it on your own; in that case, please decline the request. You can allow push notifications yourself, even at the age of 13, because they do not require consent (section 7). We do not ask for consent in the order portal. On the other pages of our website, a cookie banner asks whether you agree to analytics and marketing services; if you are under 16, please decline.

18.3 No advertising profiles, requests from parents

We do not create advertising profiles. You can exercise your rights yourself. Your parents can also contact us, for example to request information or to have your customer account deleted; to make sure that no unauthorised person receives your data, we then ask them for proof of their parental custody.

19. Changes to this Privacy Policy

19.1 Updates

We update this Privacy Policy when the app, the order portal or the law changes. If you have a customer account, we tell you about significant changes with a separate notice the next time you use the app or the order portal; you do not need to agree to the Privacy Policy. If you use the app without a customer account, you will find the changes in the box at the beginning of this Privacy Policy. You can always find the current version in the app and on our website at citychickennhas.de/en/datenschutz/kundenkonto, where it is also available as a PDF. You can request earlier versions by e-mail to media@citychicken-nhas.de.