

At Bolt, we are focused on making cities for people. As part of this mission, we intend to bring self-driving technology to Europe, to shape the next step in how people move through cities. Tallinn is our home, which is why we are taking the first steps here. In the first phase, we are focusing on real-world data collection, laying the groundwork for autonomous driving operations in a way that will respect privacy and enhance both vehicle safety and road traffic safety.

Date when this Privacy Notice was last updated: 3 March 2026

Table of Contents

1. About this Privacy Notice
2. How can you contact us?
3. What personal data do we process?
4. What purposes do we use your personal data for, and what is our legal basis for processing?
5. Who do we share your personal data with?
6. Does Bolt transfer your personal data to other countries?
7. How do we keep your personal data safe?
8. How long do we retain your personal data for?
9. Vehicle identification
10. What are your rights?

1. About this Privacy Notice

This Privacy Notice ("**Notice**") describes how Bolt Operations OÜ ("**Bolt**", "**We**" or "**Us**") collects and uses any personal data that may be captured by our limited number of (driver-operated) data collection vehicles ("**Vehicles**"), which have been deployed to collect information on road traffic conditions in order to research and develop autonomous driving systems in Tallinn, Estonia. More information about Bolt and its group companies is set out [here](#).

The term "**you**" or "**your**" refers to persons whose personal data may be captured by the Vehicles when driving on public roads. This Notice lets you know how we promise to look after your personal data and tells you about your privacy rights and the choices and controls available to you.

This Notice focuses on the original collection of recordings and their subsequent use for researching and developing autonomous driving systems. This Notice does not concern data processed during journeys conducted by autonomous vehicles.

2. How can you contact us?

Bolt is the data controller of your personal data processed under this Notice. We have appointed a Global Data Protection Officer and an Office of the Data Protection Officer Team who can be contacted by emailing our Privacy Mailbox at privacy@bolt.eu.

3. What personal data do we process?

We have equipped a limited number of Vehicles with various sensors (cameras, LiDARs, radars) which perceive the surroundings of the Vehicles and gather real-world information from public roads, including road geometry and markings, traffic signs, location information, spatial information, motion information and other vehicles, cyclists, obstacles and pedestrians. The sensor configuration is fixed and designed to capture street-level perspectives only, without

zoom or targeted recording enabled, and does not include any collection of audio data. The focus of such data collection is on traffic conditions, and the systems are not configured to determine the identity of any persons. Nevertheless, the Vehicle cameras may incidentally record certain personal data of individuals that are in their field of view, including:

- **Facial Images.**
- **Licence Plates**
- **Other Visual Data:** Any other personal data incidentally captured on the recordings, for example vehicle model and colour.
- **Recording Metadata:** Date, time and approximate location.

The recordings are immediately processed through an anonymisation engine to automatically detect and irreversibly blur any faces and/or licence plates that have been captured, before being transmitted onto physical SSD hardware in the Vehicle and later being uploaded to our secure storage server. Additional automated checks of a subset of data are also applied to ensure that the anonymisation layer has been appropriately applied. This takes place before the recordings are used to research, validate and develop software components of autonomous driving systems, because we are only interested in technical patterns (such as object shapes, relative positions and road layout) - rather than personally identifiable information - when developing the systems to improve their accuracy at identifying what one might expect to see on the road (e.g., other vehicles, pedestrians and obstacles).

4. What purposes do we use your personal data for, and what is our legal basis for processing?

The table below sets out:

- our purposes for processing your personal data;
- our legal grounds (known as a '**legal basis**') under data protection law, for each purpose; and
- the categories of personal data we use for each purpose. Learn more about what personal data these categories include in Section 3 "What personal data do we process?" above.

Here is a general explanation of each 'legal basis' that Bolt relies on to process your personal data to help you understand the table below.

• **Legitimate Interests:** When we process your personal data based on legitimate interest grounds. This includes our commercial and non-commercial interests in providing an innovative and safe service. Where the table below states that we rely on legitimate interests, we have provided a brief description of the legitimate interest. If you would like more information about this (including the balancing test), please contact us using the methods set out in Section 2 "How can you contact us?" above.

• **Compliance with Legal Obligations:** When we must process your personal data to comply with laws or regulations in the markets we operate in, such as to comply with requests from the police or relevant local authorities.

Purpose of Processing	Legal Basis	Categories of Data
Recording Compilation and Blurring	• <i>Legitimate Interests</i> - It is in our interest to create	• Facial Images • Licence Plates

Any personal data captured incidentally by the Vehicle cameras is processed to compile datasets that are immediately put through an anonymisation engine which detects and blurs faces and/or licence plates, so that the blurred recordings can be later uploaded to our secure storage server.	real-world datasets that can subsequently be used to research and develop autonomous driving systems. It is also in the general public's interests for any faces and/or licence plates captured in such datasets to be blurred in real-time.	• Other Visual Data • Recording Metadata
Research and Development Blurred recordings are subsequently used to internally research, validate and develop software components of autonomous driving systems (such as perception, prediction and motion planning).	• <i>Legitimate Interests</i> - It is in our interest, as well as the interests of passengers and the general public, to research and develop autonomous driving systems with comprehensive real-world datasets, thereby improving the overall safety and reliability of such systems.	• Other Visual Data • Recording Metadata
Legal Proceedings and Legal Compliance Where personal data exists at the relevant time, we may process such data for establishing, exercising or defending legal claims. In some cases, we also have a legal obligation to share personal data with third parties - for example, if we receive a court order or need to cooperate with a data protection authority, or other relevant authority. We also respond to lawful requests from police or other public bodies, especially in emergencies, legal disputes, or where someone's safety is at risk. We always check that we have a lawful basis to share your data and keep a record of the	• <i>Compliance with Legal Obligations</i> - We process personal data to comply with an obligation, when there is a request from a regulator, law enforcement or other governmental body. • <i>Legitimate Interests</i> - In the context of litigation or other disputes, it is in our interest to protect our interests and rights, including as part of investigations, regulatory inquiries or litigation.	• Other Visual Data • Recording Metadata

decision.		
-----------	--	--

5. Who do we share your personal data with?

Where personal data still exists at the relevant time, we may share it with the following categories of recipients.

Category of Recipients	Description
Bolt Group Companies and Employees	We may share your personal data with our Bolt Group Companies (including Bolt local subsidiaries), who may similarly use your personal data in the manner described in this Notice. In all cases, access is restricted to authorised Bolt personnel involved in the project. Personal data is not shared with partners as part of processing.
Law Enforcement, Data Protection, Tax, Transport and Licensing Authorities and other relevant Third Parties	We may disclose information under a court order or where we cooperate with a data protection supervisory authority or a licensing authority in handling complaints or investigations. We may also share your personal data with law enforcement or other public authorities, including responding to requests when the information is required by law or furthers a public interest task. We may also share your data to other relevant third parties, including emergency services, where the information furthers a public interest task, is necessary in the context of a legal dispute, and/or someone's life is at risk. In any scenario, we will take steps to ensure that we have a lawful basis on which to share the information, and we will make sure that we document our decision.

6. Does Bolt transfer your personal data to other countries?

Your personal data is primarily processed and stored in Estonia. We operate internationally and as a result, your personal data may also be transferred to and/or processed by Bolt Group Companies and employees outside the country where you are located when undertaking the activities described in this Notice, in particular in Germany and the United Kingdom. Please see our Bolt Group Companies table for further details.

No international transfers of your personal data outside of the European Economic Areas ("EEA") are planned for this project, with the exception of occasional transfers to the United Kingdom. Nevertheless, if we transfer personal data outside of the EEA, we will make sure that we take steps necessary to comply with applicable legal requirements and rely on the following transfer mechanisms:

- **Adequacy Decisions:** We will rely on decisions from the European Commission where they recognise that certain countries and territories outside of the European Economic Area ensure an adequate level of protection for personal information. Please click [here](#) to see the list of countries deemed 'adequate' by the European Commission. We rely on these adequacy decisions when we transfer personal data we collect from the EEA to the United States (where some of our third party service providers are based).

• **Standard Contractual Clauses (SCCs):** We will utilise standard contractual clauses approved by the European Commission for transfers outside the EEA and by the UK Government for transfers outside of the United Kingdom. Please click [here](#) to see the EEA SCCs and click [here](#) to see the UK SCCs. We will rely on SCCs when we transfer personal data we collect from the EEA and the United Kingdom to the United States, Singapore and Nigeria where some of our third party service providers are based.

There may be certain situations (such as responding to law enforcement requests - see Section 4 “What purposes do we use your personal data for, and what is our legal basis for processing?” above) where a transfer of personal data will take place on the basis of exemptions provided for under applicable data protection legislation. In these circumstances, we will take steps to minimise and protect the personal data transferred.

7. How do we keep your personal data safe?

The security of your personal data is very important to us, and we have implemented appropriate technical and organisational controls to protect your personal data against unauthorised processing and against accidental loss, damage or destruction. In particular:

- Recordings are in real-time processed through an anonymisation engine to automatically detect and irreversibly blur any faces and/or licence plates that have been captured.
- Raw (un-blurred) versions of the recordings are immediately and permanently deleted from Bolt’s systems once blurred versions have been generated.
- Recordings are stored on physical SSD hardware in the Vehicle before being manually uploaded to Bolt’s secure servers via an access-controlled station.
- Recordings are encrypted in transit and at rest.
- Access to our secure servers is continuously monitored to detect and prevent misuse and unauthorised disclosure.
- Any personal data collected in the course of providing Bolt Services is transferred to and stored in our data centres which are located within the EEA. Only authorised employees of Bolt group companies and partners have access to the personal data and they may access the data only for the purpose of resolving issues associated with the use of the services (including disputes regarding transportation services and customer support services in the respective countries <https://bolt.eu/cities/>).

8. How long do we retain your personal data for?

We keep your personal data only as long as is necessary for the purposes described above. We have listed below the specific retention periods that apply to the personal data we process about you.

Category of Retention Period	Description
Processing of raw recordings	Once a raw recording has been captured by a Vehicle camera, it will be immediately processed through an anonymisation engine to automatically detect and irreversibly blur any faces and/or licence plates that have been captured. The original raw recordings will then be immediately and permanently deleted.
Processing of blurred	We retain the blurred recordings for 5 years, as is necessary

recordings	to validate and develop software components of autonomous driving systems to an appropriate safety standard. Where we need to retain curated sections of the recordings for longer periods as validation datasets, we aim to ensure that such datasets do not include any information that can be used to directly identify individuals.
Formal investigations and disputes	Where personal data still exists at the relevant time, we retain it where necessary for a formal investigation by a relevant authority or in the event of a legal dispute, until the investigation or dispute is satisfied or expired.

9. Vehicle identification

The Vehicles are marked with a sticker to ensure that you are notified about relevant information at the moment of data collection. For example: [sticker](#)

10. What are your rights?

You have various rights under applicable data protection laws. However, in the context of personal data that are processed for the specific purposes set out in this notice, please note that these rights are necessarily qualified by the following:

- Any facial images and/or licence plates captured in the recordings will be immediately and permanently blurred, such that they are no longer identifiable.
- Bolt neither collates nor indexes any personal data that is incidentally captured in the Vehicle recordings. As a result, it is highly unlikely that we will be able to identify relevant personal data on our systems (in response to a data subject rights request) unless you provide supporting information that would allow us to identify the recording sections(s) (such as location, date and time). Please note that even with this supporting information, we may not be able to verify your identity and/or the relevant recording section(s), given that our systems are not configured to determine the identity of any persons captured in the recordings.

Nevertheless, Bolt will consider the following rights requests on a case-by-case basis (where applicable):

- **Access your personal data (known as “Right of Access”)**: You have the right to access and to request copies of your personal data.
- **Update/correct your personal data (known as “Right of Rectification”)**: You have the right to request us to correct personal data that is inaccurate or incomplete.
- **Delete your personal data (known as “Right of Erasure”)**: You have the right to request that we erase your personal data, under certain conditions. Personal data that is processed pursuant to a legal obligation or where we have an overriding legitimate interest may not be deleted upon request.
- **Restrict use of your personal data (known as “Right to Restrict Processing”)**: You have the right to request that we restrict the processing of your personal data, under certain conditions.
- **Object to use of your personal data (known as “Right to Object”)**: You have the right to object to our processing of your personal data, under certain conditions (e.g., we are processing your personal data under legitimate interests). This includes the right to object to our processing of your personal data for direct marketing purposes.

- **Object to solely automated decisions being made about you which has legal or similarly significant effect on you (known as “Right to object to automated decision making”)** - The processing described in this Notice does not involve any automated decision-making, including profiling, that produces legal effects or similarly significant effects concerning individuals within the meaning of Article 22 of the GDPR. Although blurred recordings are used to research, develop and validate autonomous driving system software, this processing is not used to make decisions about identifiable individuals, does not evaluate personal characteristics, and does not result in any action, decision, or outcome that affects a specific person.
- **Port your personal data (known as “Right to Data Portability”)**: You have the right to request that we transfer the personal data that you have given us to another organisation, or directly to you, under certain conditions. This only applies to information you have given us. As the recordings are collected passively in public spaces, the right to data portability does not apply to this processing.
- **File a complaint**: If you have any concerns regarding the processing of your personal data, you have the right to lodge a complaint with the Estonian Data Protection Inspectorate (“AKI”) who is our lead supervisory authority or your local data protection authority. You can find their contact details on their websites. You may also have a right to seek a judicial remedy.

To exercise any of the above rights, you can also contact the Office of the Data Protection Officer Team by emailing our Privacy Mailbox at privacy@bolt.eu.