Wolt

Security and Privacy Whitepaper

2023

1. Introduction

Wolt is a technology company known for its online food and grocery delivery platform. Wolt's mission is to make cities better places for customers, merchants and couriers alike. Wolt's platform makes it easy for customers to order whatever they need on one app, for merchants to make additional sales, and for couriers to make meaningful earnings flexibly. To enable this, Wolt is developing a wide range of technologies from local logistics to retail software and financial solutions, as well as operating its own grocery stores under the Wolt Market brand.

Wolt is – essentially – building new infrastructure. We're building a connection between restaurants and retailers that want to make and sell food and other products, couriers that want to earn through delivering those products, and customers who want to free up time and effort to focus on the more important things in life.

By doing this, we are also making our cities better places to live. And by "better" we mean happier people: happier small enterprises that have more business and that can employ more people, happier couriers that have a flexible way to earn when they choose, happier customers who now have easy access to a great meal or anything else they need, exactly when and where they need it - and who get to save some of their precious time while they are at it.

2. Our vision: Privacy and security are built in with every Wolt order

Security as an enabler

The responsibility of any security team is to protect the existing business as well as future business from all imaginable threats. However, in order to be effective, it is important for a security team to have a strong understanding of the organization's business goals and objectives.

Understanding the organization's business focus allows the Security team to align their efforts with the organization's overall strategy. This means identifying and prioritizing initiatives that are most critical to the organization's success, and developing security measures that support these goals.

At Wolt, security is viewed as an enabler rather than a hindrance. The mindset is one of proactive risk management, where security is an integral part of the business strategy.

This approach has created a culture of trust and collaboration, where security is not seen as a burden, but rather a necessary component of success. The organization proactively does risk assessments to identify potential threats and weaknesses and implements measures to mitigate them. By using this approach, Wolt has been able to respond to new threats and emerging risks quickly and effectively, rather than reacting after the fact.

We believe that as a result of this mindset, Wolt has become a more agile, innovative, and resilient organization. We are able to embrace new technologies, business models, and revenue streams, while mitigating the risks associated with these changes.

Initiatives that we're proud of

We wanted to highlight some of the cool things we've done to make our products and services more secure during the past few years. This chapter is all about initiatives we're proud of, and how they've made a real difference in keeping our employees' and stakeholders' data safe.

Passwordless and Passkeys
Does anyone like passwords? We certainly don't. We firmly believe that security should go hand in hand with great user experience, which is why in 2021 we made the decision to get rid of password login for customer-facing apps and replace them with a magic link login. We've also made an effort to enforce SSO (Single-Sign On) in the majority of our internal SaaS tools and this remains a criterion in the vendor onboarding pipeline as well.

During 2023, our goal is to have every Wolt employee enrolled in phishing-resistant authentication methods, primary of which is Passkey Authentication. Passkey Authentication is a new authentication method that utilizes end-user devices' cryptography and biometric authentication to serve as a second factor instead of SMS tokens or time-based one time passwords (TOTP). Using passkeys together with session protection controls greatly mitigates the risk of most phishing attacks. Read more about Passkeys from the FIDO alliance.

Access management in OpsTools
OpsTools are a set of internal tools that serve the operational needs of our support function, courier and country operations as well as finance and merchant operations. If AWS is the brain of Wolt, OpsTools are definitely the heart - they're basically our own home-grown ERP.

A lot of effort has been put into hardening OpsTools into the tool it is now - all user roles and access levels have been designed from the ground up in order to fit the needs of the business, as well as to protect the data of our customers, couriers and merchants.

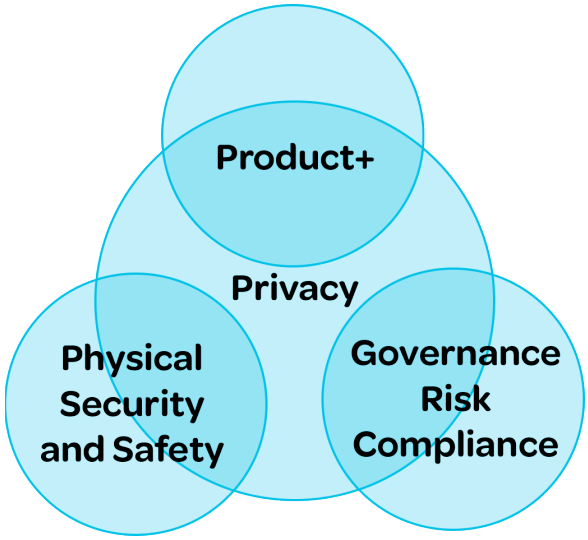
Next-gen physical access control
We're always conscious of the effectiveness of security methods we want to deploy to our employees and try to avoid any "security theater". Early on we decided to not go with the traditional badge-style access control, which is why we've started deploying OpenPath as our physical access control system in our premises.

OpenPath is a keyless door access control system that utilizes Bluetooth and WiFi in our smartphones to grant access to our employees when they enter our premises. We've also planned to have an integration to our Courier app in order to grant time-based access for couriers entering our Wolt Markets during deliveries. No more re-keying of locks or missing key fobs!

Security Hero Award
The Security Hero Award is a formal way for us to celebrate our colleagues who have helped us in security, privacy, or safety related projects, or have been otherwise proactive in promoting secure ways of working at Wolt. Every month each team member can nominate people that they deem to be deserving of the award - a shiny "challenge coin" with our team mascot, Security Yuho on it! The nominees with the most votes will receive the coin as well as praise in a company-wide Slack post.

Our dedicated Security team
While Wolt started its journey in 2014, the Security team within it is relatively new. Our first dedicated team members started in 2020 and the team has grown into a versatile group of about a dozen professionals in the past few years. We've divided our work into three main focus areas: Product Security, Physical Security and Safety and GRC (Governance, Risk and Compliance). These are glued together with privacy, since it encompasses everything we do in the Security team.

Wolt's product teams operate in an autonomous model - each autonomous team can agree upon the ways of working that work best for them, while respecting Wolt values and contributing to the overall roadmaps of the company. This is also true for the Wolt Security team. We are an independent unit that reports directly to the CEO.



3. Data protection

Privacy and security overview
Privacy and security are at the heart of Wolt. We value the privacy of our customers and partners as well as employees, and want to ensure Wolt is secure to use and available at all times. We want to make sure that our customers and partners have a great experience that is secure, reliable and respects their privacy.

For us privacy is not a pure compliance requirement or something that is just "the right thing to do". By respecting and complying with privacy requirements we are able to create a positive impact, evoke a feeling of trust and create stronger relationships with everyone whose personal data we process.

We are firm believers of Privacy by Design and Privacy by Default. In practice this means we aim to ensure that privacy is taken into account already at the planning stage of a new product, service or other processing operation. This helps us to ensure that privacy is not an afterthought, but rather that the individuals' privacy is really on our mind when building up something new or amending existing offerings or operations.

We comply with the GDPR & other applicable laws

As a company headquartered in Finland, the EU General Data Protection Regulation (GDPR) sets a legal standard for our privacy practices. In addition we comply with all other applicable local privacy rules. We follow authoritative guidance and regulatory development in this field very closely and align our practices respectively.

We have established a privacy program ensuring the high privacy maturity of our practices. We assess and review our practices regularly and develop them further to ensure protection of privacy under all circumstances. We also train our employees on a regular basis on privacy and security matters to ensure awareness.

Wolt is a "data controller" for personal data on its platform. This means we define the purposes and means for the specific personal data processing operations. As a controller, we will be responsible for compliant personal data processing. We are committed to ensuring that any personal data we process is processed only for the specific purpose in accordance with our applicable privacy statements.

In addition, we also have Wolt Drive API and eCommerce delivery as a service models where we are a "data processor". This means that in such a case we will not process personal data for any other purposes than to fulfill the order and the contractual obligations with the client in accordance with the agreed data processing agreement.

Irrespective of the service and our privacy legal role therein, we constantly aim to limit the personal data to the very minimum that is required for the service and purpose in question.

Wolt Enterprises Oy has also named a data protection officer that independently monitors our compliance, serves and supports us in privacy matters and fulfills other requirements in accordance with the GDPR.

Limited data flows & vendor management process

We do not transfer or disclose personal data to anyone without a prior assessment and appropriate justification. We are on top of data flows on our platform. We have a rigorous vendor onboarding and management process in place.

This way we ensure that all our subcontractors and subprocessors comply with our privacy requirements and applicable legal rules.

Data subject's rights respected

We respect individuals' legal rights and provide them easy, secure and privacy-friendly ways to ensure they can access their data or execute their other legal rights. Also, we can always be contacted and are happy to help with privacy related matters.

4. Infrastructure overview

Cloud native approach

At Wolt, we prioritize security in everything we do, including our infrastructure. We use cloud services, specifically Amazon Web Services (AWS), to take advantage of their built-in security features, scalability, and flexibility. We follow AWS best practices to ensure the security of our cloud operations.

We use infrastructure as code tools to automate and manage our infrastructure in a version-controlled, repeatable way. We also have a change management process in place to ensure that any changes to our infrastructure are reviewed and approved before deployment. The product teams are responsible for defining their own services' infrastructure (see the section on Product Security.)

We also utilize the self-healing capabilities of the cloud, including AWS Availability Zones and auto-scaling to provide a secure and reliable platform for our customers. We continuously monitor and improve our security posture to stay ahead of emerging threats and ensure that our customers can trust us with their sensitive data.

Utilizing Zero Trust

At Wolt, we don't have a typical corporate network, where plugging in or connecting to WiFi means you have access to systems that are otherwise not accessible through any other Internet connection. From a security perimeter perspective, our office network is treated the same as any other network; completely untrusted. As there is no "trusted" network to tunnel into, we don't use a traditional VPN either.

Access to internal resources is granted based on role and work needs. For example, our engineers don't all have access to our production databases. When they require access, they need to request the access individually and provide a justification for their request.

5. Product Security

The relationship of architecture and software development processes

Wolt is built on individual services built by autonomous teams (a microservice architecture). Due to the individual services' differences (e.g., architectural location, languages and frameworks, and usage scenarios), their threat models and attack surface differ. Wolt's autonomous teams have agency over their approach to security, within the boundaries of our policies such as the Data Policy. For the most common security needs, Wolt provides a number of software security related services centrally that are made available to all teams. These are discussed in more detail below.

The architecture itself supports secure development by naturally segregating parts of the architecture behind application interfaces (APIs). Many foreseeable types of attacks would only directly impact one part of the service, and service separation allows us to design for enforced separation, e.g., in terms of network connectivity.

Security in product management

Wolt's software security approach begins with product management. Product Owners will be able to determine high-level security risks, and also consider privacy compliance and physical safety aspects if relevant, already during the product concepting and UX/service design. The Wolt Security team supports Product Owners with both a risk identification framework and risk identification activities.

New Product Owners are provided with training in software security and privacy compliance.

Security in development and operations

The actual software implementation and development process is based on DevOps, meaning that the product teams have responsibility not only for developing but also deployment and operations of their systems. The deployment pipeline is automated as much as possible, which allows us to offer centralized security services (see below). The infrastructure is managed as code, so it is version controlled and benefits from similar quality checks as program code (see the section Infrastructure Overview).

The Security team supports the development teams in architectural, design-level and implementation-level security and privacy compliance questions on request.

Wolt has a mature culture for incident root cause analysis, including non-security related incidents, which ensures that the root causes are found out, documented, and lessons learned are shared with the product teams.

Security can also be viewed as an aspect of quality. Wolt has a Quality Assistance team whose members are embedded in the development teams. The Quality Assistance team coaches the developers towards adopting quality assurance practices such as team-specific quality criteria. New employees working in product development get awareness training both by the Quality Assistance and Security teams.

Application Security

Wolt's products and services are built with security in mind. Development teams are empowered, encouraged and supported to discover and document possible security threats throughout their development process in an iterative fashion; in particular throughout the design stages before any code is written. This may take the form of a threat modeling session, which the security team can facilitate.

Production code is placed under version control, for which an industry-leading collaborative platform is used. This platform allows the security and development teams to have visibility on metrics representing the code's quality and security. Such metrics are produced by a variety of tools that teams can choose depending on their product's technology stack.

These tools may automatically subject the code to linting, security anti-pattern scans, static application security testing and to software composition analysis enriched with CVE information. Additionally, the aforementioned version control platform allows teams to consciously review and judge their own code before it's integrated to the codebase. Critical repositories are subject to the four-eyes-principle before any code is integrated.

In an effort to achieve seamless collaboration with development teams, the security team strives to adapt to their existing practices, such as using the same defect-tracking tool across Wolt. This allows for a developer-oriented vulnerability management process without much overhead. In cases where the security team takes full ownership of security defects, the same defect-tracking tool is used to track the lifecycle of the defect.

To complement our existing automated efforts to find security defects, development teams are encouraged to request technical security testing from the security team or from external consultancy companies, where such audits may be executed in a white-box fashion. Additionally, Wolt runs a security bug bounty program, where we encourage ethical hackers to report any security bugs to us in exchange for monetary rewards.

Security operations and incident management

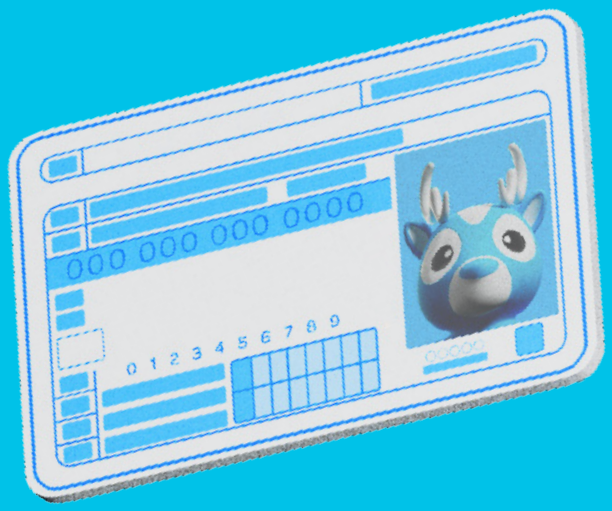
We believe that an unmonitored system cannot be secure. We have extensive system and application logging in place, aided by advanced observability into the metrics and overall health of our platform. Security-critical logs are collected into a SIEM system which alerts us about undesirable behavior. Our alerts are tested and verified against real-world scenarios. Data ingestion to the SIEM is automatically verified and an alarm is raised if a log source suddenly stops sending in data.

We know that despite all our precautions, security incidents are unavoidable, so we run regular incident simulation exercises with variable scenarios tailored to us by external partners. We train our personnel in responding to incidents, including the employees outside the security team most likely to be the first line of response.

Our security infrastructure is deployed following the same infrastructure as code principle as all of our production infrastructure. This also allows us to use the same static and dynamic analysis tools we use to ensure the security of the rest of our infrastructure.

6. Physical Security and Safety

Wolt operates in an environment that covers various premise types, for example offices, Wolt Markets and warehouses and storage units. The challenge for the Physical Security and Safety focus area is to provide input in a way that not only enhances general safety but also helps in work efficiency. The aim of the team is to do all this in an enabling way.



Three main pillars

The Physical Security and Safety focus area is run on three main pillars: regulatory compliance, incidents and risks, and culture.

Regulatory compliance is achieved by monitoring the local and EU level legislative landscape with the help of our Legal team and abiding by fire codes and other requirements. Break-ins and fires do happen, which is why we're also helping the local teams to proactively mitigate risks and avoid incidents that influence operational efficiency. The importance of culture at Wolt cannot be emphasized enough. We are a building world class company where security and safety need to be at its core, whilst not contradicting the culture of the company.

Supporting global expansion

Wolt is currently operating in 25 countries with more country launches on the horizon. We are supporting the local Wolt teams with the security and safety designs of their premises while also understanding the expansion strategy and structure globally. At Wolt we aim to do things in a way where we bring efficiency through safety and security and give everyone in the company the chance to bring their ideas to the table.

In a hyper-growth environment, security or safety cannot be a speed bump on the road to efficiency. We're working actively with the expansion team to integrate the security and safety design processes to the expansion plan. This means taking ownership of key security systems work and monitoring installations with the help of contractors.

7. Governance, Risk and Compliance (GRC)

The Governance, Risk and Compliance (GRC) focus area is responsible for advising, designing and introducing new policies, controls and security related procedures to relevant stakeholders at Wolt. We're also managing business continuity, risk and compliance programs to ensure the improvement of business resilience.

Risk management

We work closely with our Risk management team to build a realistic risk landscape for the whole of Wolt and we own most of the security controls we've implemented. We're focused on the existential risks of Wolt - threats that can realistically stop our business. These existential risks are typically related to the availability of our platform, data breaches or the compromise of our financial systems.

Our vision for approaching security control design might be a bit different from other organizations: we don't adopt industry standards blindly, instead we try to think what's smart for us and prioritize development projects that have the biggest impact for risk reduction at Wolt.

Identity and access management

Wolt's Identity and Access management is based on 'Least Privilege' and 'Segregation of Duties' principles. This means that at Wolt, employees are able to access information based on their role and duties. These principles cover all company assets and information such as customer PII, merchant financial data and courier partner data. The principles are being executed based on Wolt's Identity and Access management policy.

Internal authentication is done through SSO which Wolt has implemented to all tooling and applications that Wolt utilizes in its operations. Employee authentication is done by using phishing resistant and passwordless login, e.g. Passkey Authentication. Externally available services Wolt provides to its customers are too accessible with passwordless login methods, either by Magic Link and API Token or by using 3rd party IdP such as Google, Apple and Facebook.

Compliance requirements

Wolt undergoes periodical verifications and audits of its privacy and security practices performed by independent assessors to demonstrate that we follow industry best practices according to the requirements. See chapter 9 (Third party certifications) for more information.

Security awareness

Keeping our employees aware and vigilant about security topics is a key part of our daily life at Wolt. All our employees attend a security awareness session as a part of their onboarding process. We've also created bespoke eLearning training for information security as well as a safety training course for our Wolt Market employees.

We're also created a Digital Self-Defense Compendium - a three-level course of instructions and videos on how to improve their security posture beyond what Wolt has enforced. The compendium includes guidelines on various topics, such as computer security, mobile security, hardening social media accounts and much more.

Third party management

Effective third-party management is crucial for Wolt's security program. We rely on third-party vendors for various services and products, but we recognize that they can pose significant risks to our security posture.

To mitigate these risks, we've implemented a vendor pipeline process that includes identifying, evaluating, selecting, and onboarding vendors. During the evaluation phase, we assess the vendor's security maturity level as well as their overall risk level. We've implemented a gate where invoices are not processed unless the vendor has been formally approved.

We also conduct regular critical vendor reviews to ensure our vendors meet our security requirements and manage security risks. We've identified a list of critical vendors that are key to the function of our business. We regularly meet with these vendors and sync on topics relating to information security, privacy and their overall performance.

8. How we use data

At Wolt, we are all committed to using data in ways compliant with our policies, following the law and being ethical and respectful towards our customers and other parties, such as courier partners and venue owners and employees. For specific and up-to-date information, please refer to our Privacy Statement.

For contractual and legal reasons

We process personal data only to the extent necessary and appropriate for the specific processing purposes. As mentioned in our Privacy Statement, we collect User Data and Usage Data in order to fulfill our contractual obligations and ensure compliance with our legal obligations.

For merchants and couriers, we enforce KYC/KYB (Know Your Customer / Business) processes in order to combat money laundering and screen for individuals or organizations that are internationally sanctioned. We also monitor other fraudulent activities on our platform, such as voucher and promo code abuse as well as account takeovers and bot account creation.

To serve our customers, couriers and merchants

Wolt takes pride in world class customer service and we've always been highly rated compared to our competitors in that respect. In order to perform customer service tasks, we process relevant data in order to provide the best customer experience.

For business development and analytics

We collect only the necessary amount of information about our users, their purchases and behavior on our platform in order to improve our service. As a growth company, it's critical for us to monitor the performance of our business verticals via multiple metrics that we compose from the data retrieved from our data lake. This information is processed on our analytics platform to aid in developing our business.

We've implemented security controls and information barriers in order to limit the personal data and business information exposed to our employees.

Law enforcement data requests

We regularly cooperate with local law enforcement agencies to comply with data requests relating to criminal investigations. Data requests must always be linked to ongoing investigations and must be appropriately limited to specific activity, time and place. For more information on personal data handling, please refer to chapter 3 (Data protection).

9. Third party attestations

As a part of our goal to be a trusted partner of our customers, merchants and couriers, we've strived to acquire industry standard certifications that prove that we're worthy of their trust. As a part of DoorDash's acquisition of Wolt, we're also in the process of getting compliant with SOX (Sarbanes-Oxley) auditing and financial regulations.

PCI DSS compliance

Wolt is a Level 1 Merchant and as such, is subject to external PCI DSS compliance review on annual cadence. Currently we're still certified against version 3.2.1 but we're preparing for version 4.0.

Security testing

At Wolt, we perform both external and internal security testing. Internal testing is conducted with our own resources. Internal security testing includes, e.g., exploratory security testing, reverse attack path mapping and attack surface scanning. For external testing, we have a bug bounty program and we engage with an external security consultancy on an annual cadence to conduct a breadth-first test of our attack surface.

SOX compliance

Even if it's not your typical third party attestation, we think it counts. Everyone who is working for a US publicly traded company feels the same. This has major implications to the way you manage your IT environment and as a product company, this is at the very core of our whole business. We have implemented a series of so-called IT general controls to standardize ways of conducting internal controls related activities such as user access provisioning and deprovisioning, user access control reviews and change management procedures.

ISO 27001:2013 certification

Wolt achieved a major milestone in September 2022 when Nixu Certification Oy officially certified Wolt's Information Security Management System (ISMS) against the ISO 27001:2013 standard criteria. This is a big deal for us for many reasons, primarily because we're one of the first companies in our industry to acquire this certification. Learn more about our certification journey in our blog post.

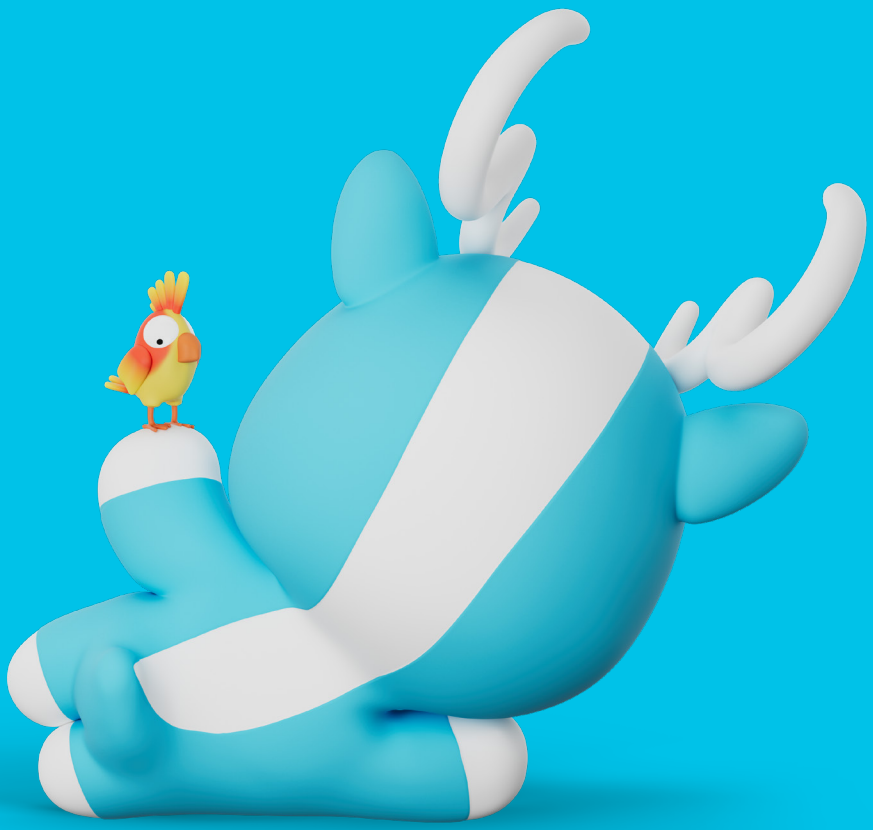
Wolt's certified ISMS covers our Product+ organization including, e.g. product development, platform development, engineering and associated support teams: Security, IT, People, Risk Management and Legal. Offices in scope are Finland (Helsinki, HQ), Sweden (Stockholm), Estonia (Tallinn), Germany (Berlin), Denmark (Copenhagen) and Japan (Tokyo).

Contact details

Please contact our customer service through the chat in our applications or **support@wolt.com**, with any security or privacy issues relating to Wolt customer or partner accounts. Our customer service will also help you with questions about data protection and requests under the EU GDPR and other national legislation. The Data Protection Officer and our privacy engineering can be contacted at **privacy@wolt.com.**

Reports of weaknesses or vulnerabilities in our services can be reported directly to the Wolt Security team at **security@wolt.com.** Our vulnerability reward program is hosted on Intigriti. You can find our security contact details, including PGP keys, in our security.txt file.

For non-urgent questions about our physical safety and security, please contact **safety@wolt.com.**



Wolt