INITIAL DISCLOSURE DOCUMENT

Last review: April 2025
Uncontrolled if accessed from sources other than pod-point.com/legal/policies

This information relates to the activities undertaken by Pod Point Limited

The Financial Conduct Authority

The Financial Conduct Authority (FCA) is the independent watchdog that regulates financial services. Use this information to decide if our services are right for you.

Treating Customers Fairly

Our business is committed to treating our customers fairly and ensuring our products and services are suitable for their needs. Treating Customers Fairly (TCF) is a core part of our culture and philosophy and you can review our commitment to it by asking for a copy of our TCF policy statement.

What products do we offer?

We are a credit broker not a lender. We can only introduce you to Klarna Bank AB (publ) FRN: 536065 who may be able to assist you with your finance requirements.

Other finance facilities

You may be able to obtain funding for your purchase from other providers and you are encouraged to seek alternative quotations and details of their products by researching on the high street, in the media and online.

What will you have to pay to us for this service?

You will not make any payment to us for processing a finance application or for introducing you to Klarna Bank AB. All charges that you will pay including, interest, documentation fees or rentals, where applicable, will be clearly shown on the finance agreement.

Commission disclosure

We do not receive any commission for introducing customers to Klarna Bank AB.

Understanding our products and documents

If you have any health issues, difficulty in understanding information or there any recent life events that could affect your ability to fully understand the information and documentation you are presented with or what your commitments are under the finance

agreement, you should carefully consider the amount of time you require to review the documentation. You should also consider if it is advisable for you to have someone you know help you make your decision. Please advise us accordingly if this is the case and we can then proceed with your requirements in the most appropriate way.

You should make sure you have sufficient time to assess the information given to ensure the funding option offered is suitable for you and meets your requirements. You should seek further explanations and ask questions if needed to fully understand the documents you are given.

Affordability

You should assess the monthly payments you are required to make throughout the agreement and ensure you are able to meet these obligations and other obligations you already have without suffering undue hardship. If you are aware of any future events that will affect your ability to meet these payments, you should ensure Klarna Bank is informed immediately.

Your credit rating could be adversely affected if you do not make payments when due which could make it harder or more expensive for you to access finance facilities in the future.

Who regulates us?

Pod Point Limited is an Appointed Representative of Product Partnerships Limited which is authorised and regulated by the Financial Conduct Authority; registration number 626349. Product Partnerships Limited's address is Second Floor, Atlas House, 31 King Street, Leeds, LS1 2HL and its permitted business is to act as a Principal for a network of firms who carry out consumer credit activities.

You can check this information on the FCA register by visiting

www.fca.org.uk/register or by contacting the FCA on 0800 111 6768.

What to do if you have a complaint

If you would like to know how we handle complaints, please ask for a copy of our complaints handling process. If you wish to register a complaint, you can contact us at **complaints@pod-point.com** or in writing at 222 Gray's Inn Road, London, WC1X 8HB.

If you can't resolve a complaint with us, we are an Appointed Representative of **Product Partnerships Limited** (FRN: 626349) and you can refer your complaint to them as our Principal firm. In writing: Product Partnerships Limited, Second Floor, Atlas House, 31 King Street, Leeds, LS1 2HL, by phone: 01274 921234, by email: **info@productpartnerships.com**

If you can't resolve a complaint with us, you may be able to refer it to the Financial Ombudsman Service whose contact details are set out below:

In writing: The Financial Ombudsman Service, Exchange Tower, London E14 9SR By telephone: 0800 0234567

By email: **complaint.info@financial-ombudsman.org.uk**

Website: **www.financial-ombudsman.org.uk**

1. Introduction

Pod Point is one of the UK's leading providers of electric vehicle charging. We believe that travel shouldn't damage the earth and our mission is to put an electric vehicle chargepoint everywhere you park. Keeping our products secure is key to this mission.

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to Pod Point. We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and always acting in compliance with it.

A vulnerability is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack. They can occur through flaws (unintended functionality), features or user error, and attackers will look to exploit any of them, often combining one or more, to achieve their end goal.

We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

2. Reporting

If you believe you have found a security vulnerability, please submit your report to us using the following email: **security@pod-point.com**

In your report, please include details of:

- The website, URL, IP or page where the vulnerability can be observed.
- A brief description of the type of vulnerability, for example, “XSS vulnerability”.
- Steps to reproduce. These should be a benign, non-destructive, proof of concept.

This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as subdomain takeovers.

3. What to expect

After you have submitted your report, we will respond to your report within 5 working days and aim to triage your report within 10 working days. We'll also aim to keep you informed of our progress.

Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to inquire about the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation.

4. Guidance

You must not:

- Break any applicable law or regulations.
- Access unnecessary, excessive or significant amounts of data.
- Modify data in Pod Point's systems or services.
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests.
- Disrupt Pod Point's services or systems.
- Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with "best practice", for example missing security headers.
- Submit reports detailing TLS configuration weaknesses, for example "weak" cipher suite support or the presence of TLS1.0 support.
- Communicate any vulnerabilities or associated details other than by means described in the published security.txt.
- Social engineer, 'phish' or physically attack Pod Point's staff or infrastructure.
- Demand financial compensation in order to disclose any vulnerabilities.

You must:

- Always comply with data protection rules and must not violate the privacy of the Pod Point's users, staff, contractors, services or systems. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services.

- Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).

5. Legalities

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause Pod Point or partner organisations to be in breach of any legal obligations.